15. 3. 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

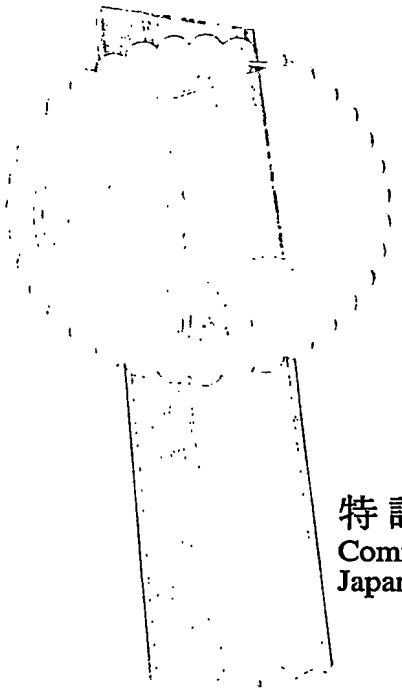
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月１７日

出願番号
Application Number: 特願２００３－０１０１８３

[ST. 10/C]: [ＪＰ２００３－０１０１８３]

出願人
Applicant(s): 加藤　誠



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００４年　３月　４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０１６８２７

【書類名】　特許願
【整理番号】　P10420T0
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　H09C　1/00
　　H04L　9/00
【発明者】
　【住所又は居所】　東京都葛飾区東金町１－３６－１－１３１８
　【氏名】　加藤　誠
【特許出願人】
　【識別番号】　500400700
　【氏名又は名称】　加藤　誠
【代理人】
　【識別番号】　100088580
　【弁理士】
　【氏名又は名称】　秋山　敦
【選任した代理人】
　【識別番号】　100111109
　【弁理士】
　【氏名又は名称】　城田　百合子
【手数料の表示】
　【予納台帳番号】　027421
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0115949
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ送信システム及びデータ送信方法並びに装置

【特許請求の範囲】

【請求項１】　送信側装置から受信側装置へ第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、

前記送信側装置は、前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択する換算定数選択手段と、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化手段と、前記第１の代替値及び前記第１の換算定数を含む第１信号を生成する第１信号生成手段と、前記第３の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第２の代替値，前記第２の換算定数及び前記パターン換算定数を含む第２信号を生成する第２信号生成手段と、前記第１信号を前記受信側装置へ送信し前記第２信号を中継装置へ送信する送信手段と、を備え、

前記中継装置は、前記パターン換算定数に対応する第３の換算定数を記憶する記憶手段と、前記第２信号を受信して該第２信号に含まれるパターン換算定数を対応する前記第３の換算定数に変換して第２´信号を生成する信号生成手段と、前記第２´信号を前記受信側装置へ送信する送信手段と、を備え、

前記受信側装置は、前記送信側装置からの前記第１信号及び前記中継装置からの第２´信号を受信して前記第１信号から前記第１の代替値及び前記第１の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数及び前記第３の換算定数を読取る読取手段と、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化手段と、前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２´信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。

【請求項２】　送信側装置から受信側装置へ第１の換算定数，第２の換算定

数，第３の換算定数及び第４の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信システムであって、

前記送信側装置は、前記第１の換算定数，前記第２の換算定数，前記第３の換算定数及び前記第４の換算定数を選択する換算定数選択手段と、前記第２の換算定数及び前記第４の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化手段と、前記第３の換算定数及び第４の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第１の代替値，前記第１の換算定数，及び前記第３の換算定数又は前記第４の換算定数に対応するパターン換算定数を含む第１信号を生成する第１信号生成手段と、前記第２の代替値，前記第２の換算定数，及び前記第１信号に含まれない前記第３の換算定数又は前記第４の換算定数のパターン換算定数を含む第２信号を生成する第２信号生成手段と、前記第１信号を第１の中継装置へ送信し前記第２信号を第２の中継装置へ送信する送信手段と、を備え、

前記第１の中継装置は、前記パターン換算定数に対応する第３の換算定数又は第４の換算定数を記憶する記憶手段と、前記第１信号を受信して該信号に含まれるパターン換算定数を対応する前記第３の換算定数又は第４の換算定数に変換して第１´信号を生成する信号生成手段と、前記第１´信号を前記受信側装置へ送信する送信手段と、を備え、

前記第２の中継装置は、前記パターン換算定数に対応する第３の換算定数又は第４の換算定数を記憶する記憶手段と、前記第２信号を受信して該信号に含まれるパターン換算定数を対応する前記第３の換算定数又は第４の換算定数に変換して第２´信号を生成する信号生成手段と、前記第２´信号を前記受信側装置へ送信する送信手段と、を備え、

前記受信側装置は、前記第１´信号及び前記第２´信号を受信して前記第１´信号から前記第１の代替値，前記第１の換算定数及び前記第３の換算定数又は第４の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数及び前記第３の換算定数又は第４の換算定数を読取る読取手段と、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復

号化データ及び第２の復号化データへ復号化する復号化手段と、前記第１の複合化データと前記第２の復号化データから前記第１´信号及び前記第２´信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。

【請求項３】　送信側装置から受信側装置へ第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、

前記送信側装置は、前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択する換算定数選択手段と、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化手段と、前記第１の代替値及び前記第１の換算定数を含む第１信号を生成する第１信号生成手段と、前記第３の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第２の代替値，前記第２の換算定数及び前記パターン換算定数を含む第２信号を生成する第２信号生成手段と、前記第１信号及び前記第２信号を前記受信側装置へ送信する送信手段と、を備え、

前記受信側装置は、前記第１信号及び前記第２信号を受信して前記第１信号から前記第１の代替値及び前記第１の換算定数、前記第２信号から前記第２の代替値，前記第２の換算定数及び前記パターン換算定数を読取る読取手段と、前記パターン換算定数に対応する第３の換算定数を記憶する記憶手段と、前記読取られたパターン換算定数から前記第３の換算定数を読取る手段と、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化手段と、前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。

【請求項４】　前記暗号化手段は、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化することを特徴と

する請求項１又は３に記載のデータ送信システム。

【請求項５】　前記暗号化手段は、前記第２の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化することを特徴とする請求項１又は３に記載のデータ送信システム。

【請求項６】　前記暗号化手段は、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数を用いて前記第２の代替値へ暗号化することを特徴とする請求項１又は３に記載のデータ送信システム。

【請求項７】　前記受信側装置は、前記第１の復号化データ又は第２の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出手段を備えたことを特徴とする請求項１乃至３のいずれかに記載のデータ送信システム。

【請求項８】　前記認証手段は、前記第１の複合化データと前記第２の復号化データが一致したときに前記認証を行うことを特徴とする請求項１乃至３のいずれかに記載のデータ送信システム。

【請求項９】　前記送信側装置，前記中継装置及び前記受信側装置は、インターネットを含む通信回線網に接続されたことを特徴とする請求項１又は２に記載のデータ送信システム。

【請求項１０】　前記送信側装置と受信側装置は、赤外線方式，無線電波方式、光通信方式、有線通信方式のいずれかによって前記信号の送受信を行うことを特徴とする請求項３に記載のデータ送信システム。

【請求項１１】　送信側装置から受信側装置へ第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、

前記送信側装置が、前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択するステップと、

前記送信側装置が、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算

定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化ステップと、

前記送信側装置が、前記第１の代替値，及び前記第１の換算定数を含む第１信号を生成する第１信号生成ステップと、

前記送信側装置が、前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数に対応するパターン換算定数を含む第２信号を生成する第２信号生成ステップと、

前記送信側装置が、前記第１信号を前記受信側装置へ送信し前記第２信号を中継装置へ送信する第１送信ステップと、

前記中継装置が、前記第２信号を受信して該第２信号に含まれるパターン換算定数を対応する前記第３の換算定数に変換して第２´信号を生成する変換ステップと、

前記中継装置が、前記第２´信号を前記受信側装置へ送信する第２送信ステップと、

前記受信側装置が、前記送信側装置からの前記第１信号及び前記中継装置からの第２´信号を受信して前記第１信号から前記第１の代替値，及び前記第１の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数を読取る読取ステップと、

前記受信側装置が、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化ステップと、

前記受信側装置が、前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２´信号を受け入れる認証をする認証ステップと、を備えたことを特徴とするデータ送信方法。

【請求項１２】　送信側装置から受信側装置へ第１の換算定数，第２の換算定数，第３の換算定数及び第４の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信方法であって、

前記送信側装置が、前記第１の換算定数，前記第２の換算定数，前記第３の換算定数及び前記第４の換算定数を選択するステップと、

前記送信側装置が、前記第２の換算定数，及び前記第４の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化ステップと、

前記送信側装置が、前記第１の代替値，前記第１の換算定数，及び前記第３の換算定数又は前記第４の換算定数に対応するパターン換算定数を含む第１信号を生成する第１信号生成ステップと、

前記送信側装置が、前記第２の代替値，前記第２の換算定数，及び前記第１信号に含まれない前記第３の換算定数又は前記第４の換算定数のパターン換算定数を含む第２信号を生成する第２信号生成ステップと、

前記送信側装置が、前記第１信号を第１の中継装置へ送信し前記第２信号を第２の中継装置へ送信する第１送信ステップと、

前記第１の中継装置及び前記第２の中継装置が、前記第１信号又は前記第２信号を受信して該信号に含まれるパターン換算定数を対応する前記第３の換算定数又は第４の換算定数に変換して第１´信号又は第２´信号を生成する変換ステップと、

前記第１の中継装置及び前記第２の中継装置が、前記第１´信号又は前記第２´信号を前記受信側装置へ送信する第２送信ステップと、

前記受信側装置が、前記第１´信号及び前記第２´信号を受信して前記第１´信号から前記第１の代替値，前記第１の換算定数，及び前記第３の換算定数又は第４の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数又は第４の換算定数を読取る読取ステップと、

前記受信側装置が、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化ステップと、

前記受信側装置が、前記第１の複合化データと前記第２の復号化データから前記第１´信号及び前記第２´信号を受け入れる認証をする認証ステップと、を備えたことを特徴とするデータ送信方法。

【請求項１３】　送信側装置から受信側装置へ第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信デ

ータを送信するデータ送信方法であって、

前記送信側装置が、前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択するステップと、

前記送信側装置が、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化ステップと、

前記送信側装置が、前記第１の代替値及び前記第１の換算定数を含む第１信号を生成する第１信号生成ステップと、

前記送信側装置が、前記第２の代替値，前記第２の換算定数及び前記第３の換算定数に対応するパターン換算定数を含む第２信号を生成する第２信号生成ステップと、

前記送信側装置が、前記第１信号及び前記第２信号を前記受信側装置へ送信する送信ステップと、

前記受信側装置が、前記第１信号及び前記第２信号を受信して前記第１信号から前記第１の代替値及び前記第１の換算定数、前記第２信号から前記第２の代替値，前記第２の換算定数及び前記パターン換算定数を読取る読取ステップと、

前記受信側装置が、前記読取られたパターン換算定数に対応する前記第３の換算定数を取得する換算定数取得ステップと、

前記受信側装置が、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化ステップと、

前記受信側装置が、前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２信号を受け入れる認証をする認証ステップと、を備えたことを特徴とするデータ送信方法。

【請求項１４】　前記暗号化ステップでは、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化することを特徴とする請求項１１又は１３に記載のデータ送信方法。

【請求項１５】　前記暗号化ステップでは、前記第２の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化することを特徴とする請求項１１又は１３に記載のデータ送信方法。

【請求項１６】　前記暗号化ステップでは、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数を用いて前記第２の代替値へ暗号化することを特徴とする請求項１１又は１３に記載のデータ送信方法。

【請求項１７】　前記認証ステップの後、前記第１の復号化データ又は第２の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出ステップを備えたことを特徴とする請求項１１乃至１３のいずれかに記載のデータ送信方法。

【請求項１８】　前記認証ステップでは、前記第１の複合化データと前記第２の復号化データが一致したときに前記認証を行うことを特徴とする請求項１１乃至１３のいずれかに記載のデータ送信方法。

【請求項１９】　第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信する装置であって、

前記換算定数に対応するパターン換算定数を記憶する記憶部と、

前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択する換算定数選択処理と，前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化処理と，前記第１の代替値，及び前記第１の換算定数を含む第１信号を生成する第１信号生成処理と，前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数に対応するパターン換算定数を含む第２信号を生成する第２信号生成処理と，前記第１信号と前記第２信号をそれぞれ送信する処理と，を行う制御部と、

前記第１信号と前記第２信号を外部へ送信する送信部と、を備えたことを特徴

とする装置。

【請求項２０】　前記制御部は、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化することを特徴とする請求項１９に記載の装置。

【請求項２１】　前記制御部は、前記第２の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化することを特徴とする請求項１９に記載の装置。

【請求項２２】　前記制御部は、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数を用いて前記第２の代替値へ暗号化することを特徴とする請求項１９に記載の装置。

【請求項２３】　第１の換算定数，第２の換算定数，第３の換算定数及び第４の換算定数のうち二の換算定数によって暗号化された送信データを送信する装置であって、

前記換算定数に対応するパターン換算定数を記憶する記憶部と、

前記第１の換算定数，前記第２の換算定数，前記第３の換算定数及び前記第４の換算定数を選択する換算定数選択処理と，前記第２の換算定数及び前記第４の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化処理と，前記第１の代替値，前記第１の換算定数，及び前記第３の換算定数又は前記第４の換算定数に対応するパターン換算定数を含む第１信号を生成する第１信号生成処理と，前記第２の代替値，前記第２の換算定数，及び前記第１信号に含まれない前記第３の換算定数又は前記第４の換算定数のパターン換算定数を含む第２信号を生成する第２信号生成処理と，を行う制御部と、

前記第１信号と前記第２信号を外部へ送信する送信部と、を備えたことを特徴とする装置。

【請求項２４】　送信データの暗号化に用いられる換算定数に対応するパタ

ーン換算定数を含む信号を転送する装置であって、

前記換算定数に対応するパターン換算定数を記憶する記憶部と、

前記信号を送受信する送受信部と、

受信した前記信号に含まれるパターン換算定数を対応する前記換算定数に変換して前記信号を変換する信号生成処理と，前記変換された信号を転送する処理と，を行う制御部と、を備えたことを特徴とする装置。

【請求項２５】　第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第１信号と第２´信号を受信して送信データを復号化する装置であって、

前記第１信号には、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第１の代替値と，第１の換算定数と，が含まれ、

前記第２´信号には、前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第２の代替値と，前記第２の換算定数と，前記第３の換算定数と，が含まれ、

前記第１信号及び前記第２´信号を受信する受信部と、

受信した前記第１信号から前記第１の代替値及び前記第１の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数及び前記第３の換算定数を読取る処理と，前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化処理と，前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２´信号を受け入れる認証をする認証処理と，を行う制御部と、を備えたことを特徴とする装置。

【請求項２６】　第１の換算定数，第２の換算定数，第３の換算定数及び第４の換算定数のうち二の換算定数によって暗号化された送信データを含む第１´信号と第２´信号を受信して送信データを復号する装置であって、

前記第１´信号には、前記第２の換算定数及び前記第４の換算定数を用いて前記送信データが暗号化された第１の代替値と，前記第１の換算定数と，前記第３の換算定数又は前記第４の換算定数と，が含まれ、

前記第２´信号には、第１の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第１の代替値と，第２の換算定数と，前記第１´信号に含まれていない第３の換算定数又は前記第４の換算定数と，が含まれ、

前記第１´信号及び前記第２´信号を受信する受信部と、

受信した前記第１´信号から前記第１の代替値，前記第１の換算定数，及び前記第３の換算定数又は第４の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数又は第４の換算定数を読取る処理と，前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化処理と，前記第１の複合化データと前記第２の復号化データから前記第１´信号及び前記第２´信号を受け入れる認証をする認証処理と，を行う制御部を備えたことを特徴とする装置。

【請求項２７】　第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第１信号と第２信号を受信して送信データを復号化する装置であって、

前記第１信号には、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第１の代替値と，第１の換算定数と，が含まれ、

前記第２信号には、前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第２の代替値と，前記第２の換算定数と，前記第３の換算定数に対応するパターン換算定数と，が含まれ、

前記換算定数に対応するパターン換算定数を記憶する記憶部と、

前記第１信号及び前記第２信号を受信する受信部と、

前記第１信号から前記第１の代替値，及び前記第１の換算定数、前記第２信号から前記第２の代替値，前記第２の換算定数，及び前記パターン換算定数を読取る処理と，前記読取られたパターン換算定数から前記第３の換算定数を取得する処理と，前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化処理と，前記第１の複合化データと前記第２の復号化データから前記第１信号

及び前記第２信号を受け入れる認証をする認証処理と，を行う制御部と、を備えたことを特徴とする装置。

【請求項２８】　前記制御部は、前記第１の復号化データ又は第２の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出することを特徴とする請求項２５乃至２７のいずれかに記載の装置。

【請求項２９】　前記制御部は、前記第１の複合化データと前記第２の復号化データが一致したときに前記認証を行うことを特徴とする請求項２５乃至２７のいずれかに記載の装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ送信する際に送信データが漏洩した場合においても、その復号化が困難であると共に、第３者の成りすまし送信による不都合を回避できるデータ送信システム及びデータ送信方法並びに装置に関する。

【０００２】

【従来の技術】

従来から、送信者側で送信すべきデータの暗号化を行い、該暗号化データと該暗号化データを復号化するための暗号鍵とを別々の回線（例えば、衛星通信回線と地上回線）によって受信者側へ送信する技術がある。（例えば、特許文献１参照）。

【０００３】

受信者側では、暗号化されたデータと暗号鍵とを別々に受信し、これらにより元のデータを復号化することができる。このように別々の回線で暗号化データと暗号鍵が送信されることにより、データ送信の秘匿性を高めることができる。

【０００４】

【特許文献１】

特許第３０５２３２２号公報（第２－３頁、第１－２図）

【０００５】

【発明が解決しようとする課題】

しかし、受信者は、暗号鍵と暗号化されたデータの送信者を認証することなくデータを受信するため、本来送信するはずの送信者に成り代わって第３者によって送信されても送信データを認証することができなかった。

【０００６】

インターネット等の通信回線上においては、個人認証を行う認証サービス会社の個人認証サービスもある。しかし、そのような認証サービス会社による個人認証サービスは高価であり、個人が利用するには不向きであった。

【０００７】

本発明は、上記課題を解決するためになされたものであり、本来の送信者になりかわって第３者がデータを送信しても、受信者側で送信データの認証を行うことができ、上記成りすまし送信による不都合を防ぐことができるデータ送信システム及びデータ送信方法並びに装置を提供することにある。

【０００８】

【課題を解決するための手段】

上記課題は請求項１に記載のデータ送信システムによれば、送信側装置から受信側装置へ第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、前記送信側装置は、前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択する換算定数選択手段と、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化手段と、前記第１の代替値及び前記第１の換算定数を含む第１信号を生成する第１信号生成手段と、前記第３の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第２の代替値，前記第２の換算定数及び前記パターン換算定数を含む第２信号を生成する第２信号生成手段と、前記第１信号を前記受信側装置へ送信し前記第２信号を中継装置へ送信する送信手段と、を備え、前記中継装置は、前記パターン換算定数に対応する第３の換算定数を記憶する記憶手段と、前記第２信号を受信して該第２信号に含まれるパターン換算定数を対応する前記第３の換算定数に変換

して第２´信号を生成する信号生成手段と、前記第２´信号を前記受信側装置へ送信する送信手段と、を備え、前記受信側装置は、前記送信側装置からの前記第１信号及び前記中継装置からの第２´信号を受信して前記第１信号から前記第１の代替値及び前記第１の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数及び前記第３の換算定数を読取る読取手段と、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化手段と、前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２´信号を受け入れる認証をする認証手段と、を備えることにより解決される。

【０００９】

このように本発明によれば、第１信号に含まれる暗号化データを暗号化した第２の換算定数は第２信号に含めて送信され、第２信号に含まれる暗号化データを暗号化した第１の換算定数は第１信号に含めて送信される。

【００１０】

さらに、第３の換算定数そのものは送信されず、第３の換算定数に対応するパターン換算定数が第２信号に含めて中継装置へ送信される。そして、このパターン換算定数が、中継装置で第３の換算定数へ変換されることにより、第２信号が第２´信号に変換され、受信側へ転送される。

【００１１】

このように送信することにより、第３者は第１信号及び第２信号の双方を取得したとしてもパターン換算定数が不明であるので、送信データの復号化を行うことはできない。また、第３者が第１信号又は第２´信号の一方を取得したとしても、それぞれの信号には換算定数のすべての換算定数が含まれていないので、復号化を行うことはできない。

【００１２】

さらに、第３者が第１信号及び第２´信号の双方を取得したとしても、復号化方法を取得しない限り、有意な復号化データを得ることはできない。

【００１３】

以上のように、本発明によれば第３者が暗号化データを不正に取得したとして

も、暗号化データの復号化を有意に行うことができず、送信データの秘匿性を高めることができる。

【００１４】

また、受信側装置では、送信側装置で選択されたパターン換算定数を知らなくても暗号化データを復号化することができる。したがって、送信側装置では複数のパターン換算定数及び換算定数の組合せを設定することにより、複数の受信側装置へ暗号化データを送信する場合にも秘匿性を高めることができる。

【００１５】

そして、第３者には換算定数による暗号化方法及びパターン換算定数が不明であるため、送信者に成り代わって送信したとしても、受信側装置では有意なデータとして復号化することができないか、復号化データが一致しないので、成りすまし送信による不都合を回避することができる。

【００１６】

また、上記課題は、請求項２のデータ送信システムによれば、送信側装置から受信側装置へ第１の換算定数，第２の換算定数，第３の換算定数及び第４の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信システムであって、前記送信側装置は、前記第１の換算定数，前記第２の換算定数，前記第３の換算定数及び前記第４の換算定数を選択する換算定数選択手段と、前記第２の換算定数及び前記第４の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化手段と、前記第３の換算定数及び第４の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第１の代替値，前記第１の換算定数，及び前記第３の換算定数又は前記第４の換算定数に対応するパターン換算定数を含む第１信号を生成する第１信号生成手段と、前記第２の代替値，前記第２の換算定数，及び前記第１信号に含まれない前記第３の換算定数又は前記第４の換算定数のパターン換算定数を含む第２信号を生成する第２信号生成手段と、前記第１信号を第１の中継装置へ送信し前記第２信号を第２の中継装置へ送信する送信手段と、を備え、前記第１の中継装置は、前記パターン換算定数に対応する第３の換算定数又は第４の換算定数を記憶する記憶手段と

、前記第１信号を受信して該信号に含まれるパターン換算定数を対応する前記第３の換算定数又は第４の換算定数に変換して第１´信号を生成する信号生成手段と、前記第１´信号を前記受信側装置へ送信する送信手段と、を備え、前記第２の中継装置は、前記パターン換算定数に対応する第３の換算定数又は第４の換算定数を記憶する記憶手段と、前記第２信号を受信して該信号に含まれるパターン換算定数を対応する前記第３の換算定数又は第４の換算定数に変換して第２´信号を生成する信号生成手段と、前記第２´信号を前記受信側装置へ送信する送信手段と、を備え、前記受信側装置は、前記第１´信号及び前記第２´信号を受信して前記第１´信号から前記第１の代替値，前記第１の換算定数及び前記第３の換算定数又は第４の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数及び前記第３の換算定数又は第４の換算定数を読取る読取手段と、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化手段と、前記第１の複合化データと前記第２の復号化データから前記第1´´信号及び前記第２´信号を受け入れる認証をする認証手段と、を備えることにより解決される。

【００１７】

このように本発明によれば、請求項１に記載の発明に加え、第１信号も中継装置を介して受信側装置へ転送される。これにより、さらにデータ送信の秘匿性が高まり、又、より効果的に成りすまし送信による不都合を排除することができる。

【００１８】

また、上記課題は、請求項３に記載のデータ送信システムによれば、送信側装置から受信側装置へ第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、前記送信側装置は、前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択する換算定数選択手段と、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，又は前記第１の換算定数及び前記第３の

換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化手段と、前記第１の代替値及び前記第１の換算定数を含む第１信号を生成する第１信号生成手段と、前記第３の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第２の代替値，前記第２の換算定数及び前記パターン換算定数を含む第２信号を生成する第２信号生成手段と、前記第１信号及び前記第２信号を前記受信側装置へ送信する送信手段と、を備え、前記受信側装置は、前記第１信号及び前記第２信号を受信して前記第１信号から前記第１の代替値及び前記第１の換算定数、前記第２信号から前記第２の代替値，前記第２の換算定数及び前記パターン換算定数を読取る読取手段と、前記パターン換算定数に対応する第３の換算定数を記憶する記憶手段と、前記読取られたパターン換算定数から前記第３の換算定数を読取る手段と、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化手段と、前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２信号を受け入れる認証をする認証手段と、を備えることにより解決される。

【００１９】

このように本発明によれば、請求項１に記載の発明と異なり、中継装置を設けることなく、中継装置が行っていたパターン換算定数を換算定数に変換する処理を受信側装置で行うように構成されている。このようにすることにより、データの秘匿性を低下させることなく、また、成りすまし送信による不都合を排除することができると共に、システムの構成を簡単化することができる。

【００２０】

また、請求項４に記載のように、前記暗号化手段は、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化するように構成することができる。

【００２１】

また、請求項５に記載のように、前記暗号化手段は、前記第２の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前

記第３の換算定数を用いて前記第２の代替値へ暗号化するように構成することができる。

【００２２】

また、請求項６に記載のように、前記暗号化手段は、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数を用いて前記第２の代替値へ暗号化すれば、成りすまし送信による２つの信号が受信側装置へ送信されてきた場合であっても、それぞれの信号を復号して得られた復号化データは不一致となるので、成りすまし送信を排除する効果が高まるので好適である。

【００２３】

また、請求項７に記載のように、前記受信側装置は、前記第１の復号化データ又は第２の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出手段を備えれば、本システムのデータ秘匿性及び成りすまし送信排除効果より、本人又は受信信号を認証して外部駆動装置を操作することができるので好適である。

【００２４】

また、請求項８に記載のように、前記認証手段は、前記第１の複合化データと前記第２の復号化データが一致したときに前記認証を行うように構成することができる。また、請求項９に記載のように、前記送信側装置，前記中継装置及び前記受信側装置は、インターネットを含む通信回線網に接続する構成とすることができる。また、請求項１０に記載のように、前記送信側装置と受信側装置は、赤外線方式，無線電波方式、光通信方式、有線通信方式のいずれかによって前記信号の送受信を行うことが可能である。

【００２５】

また、請求項１１に記載のように、本発明のデータ送信方法は、送信側装置から受信側装置へ第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、前記送信側装置が、前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択するステップと、前記送信側装置が、前記第２の換算定数，

又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化ステップと、前記送信側装置が、前記第１の代替値，及び前記第１の換算定数を含む第１信号を生成する第１信号生成ステップと、前記送信側装置が、前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数に対応するパターン換算定数を含む第２信号を生成する第２信号生成ステップと、前記送信側装置が、前記第１信号を前記受信側装置へ送信し前記第２信号を中継装置へ送信する第１送信ステップと、前記中継装置が、前記第２信号を受信して該第２信号に含まれるパターン換算定数を対応する前記第３の換算定数に変換して第２´信号を生成する変換ステップと、前記中継装置が、前記第２´信号を前記受信側装置へ送信する第２送信ステップと、前記受信側装置が、前記送信側装置からの前記第１信号及び前記中継装置からの第２´信号を受信して前記第１信号から前記第１の代替値，及び前記第１の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数を読取る読取ステップと、前記受信側装置が、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化ステップと、前記受信側装置が、前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２´信号を受け入れる認証をする認証ステップと、を備えるものとすることができる。

【００２６】

また、請求項１２に記載のように、本発明のデータ送信方法は、送信側装置から受信側装置へ第１の換算定数，第２の換算定数，第３の換算定数及び第４の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信方法であって、前記送信側装置が、前記第１の換算定数，前記第２の換算定数，前記第３の換算定数及び前記第４の換算定数を選択するステップと、前記送信側装置が、前記第２の換算定数，及び前記第４の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化ステップと、前記送信側

装置が、前記第１の代替値，前記第１の換算定数，及び前記第３の換算定数又は前記第４の換算定数に対応するパターン換算定数を含む第１信号を生成する第１信号生成ステップと、前記送信側装置が、前記第２の代替値，前記第２の換算定数，及び前記第１信号に含まれない前記第３の換算定数又は前記第４の換算定数のパターン換算定数を含む第２信号を生成する第２信号生成ステップと、前記送信側装置が、前記第１信号を第１の中継装置へ送信し前記第２信号を第２の中継装置へ送信する第１送信ステップと、前記第１の中継装置及び前記第２の中継装置が、前記第１信号又は前記第２信号を受信して該信号に含まれるパターン換算定数を対応する前記第３の換算定数又は第４の換算定数に変換して第１´信号又は第２´信号を生成する変換ステップと、前記第１の中継装置及び前記第２の中継装置が、前記第１´信号又は前記第２´信号を前記受信側装置へ送信する第２送信ステップと、前記受信側装置が、前記第１´信号及び前記第２´信号を受信して前記第１´信号から前記第１の代替値，前記第１の換算定数，及び前記第３の換算定数又は第４の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数又は第４の換算定数を読取る読取ステップと、前記受信側装置が、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化ステップと、前記受信側装置が、前記第１の複合化データと前記第２の復号化データから前記第１´信号及び前記第２´信号を受け入れる認証をする認証ステップと、を備えるものとすることができる。

【００２７】

また、請求項１３に記載のように、本発明のデータ送信方法は、送信側装置から受信側装置へ第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、前記送信側装置が、前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択するステップと、前記送信側装置が、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化ステップ

と、前記送信側装置が、前記第１の代替値及び前記第１の換算定数を含む第１信号を生成する第１信号生成ステップと、前記送信側装置が、前記第２の代替値，前記第２の換算定数及び前記第３の換算定数に対応するパターン換算定数を含む第２信号を生成する第２信号生成ステップと、前記送信側装置が、前記第１信号及び前記第２信号を前記受信側装置へ送信する送信ステップと、前記受信側装置が、前記第１信号及び前記第２信号を受信して前記第１信号から前記第１の代替値及び前記第１の換算定数、前記第２信号から前記第２の代替値，前記第２の換算定数及び前記パターン換算定数を読取る読取ステップと、前記受信側装置が、前記読取られたパターン換算定数に対応する前記第３の換算定数を取得する換算定数取得ステップと、前記受信側装置が、前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化ステップと、前記受信側装置が、前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２信号を受け入れる認証をする認証ステップと、を備えるものとすることができる。

【００２８】

また、請求項１４に記載のように、前記暗号化ステップでは、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化するようにできる。

【００２９】

また、請求項１５に記載のように、前記暗号化ステップでは、前記第２の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化するようにできる。

【００３０】

また、請求項１６に記載のように、前記暗号化ステップでは、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数を用いて前記第２の代替値へ暗号化するようにできる。

【００３１】

また、請求項１７に記載のように、前記認証ステップの後、前記第１の復号化データ又は第２の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出ステップを備えれば好適である。

【００３２】

また、請求項１８に記載のように、前記認証ステップでは、前記第１の複合化データと前記第２の復号化データが一致したときに前記認証を行うようにできる。

【００３３】

また、請求項１９に記載のように、本発明は、第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信する装置であって、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記第１の換算定数，前記第２の換算定数及び前記第３の換算定数を選択する換算定数選択処理と，前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化処理と，前記第１の代替値，及び前記第１の換算定数を含む第１信号を生成する第１信号生成処理と，前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数に対応するパターン換算定数を含む第２信号を生成する第２信号生成処理と，前記第１信号と前記第２信号をそれぞれ送信する処理と，を行う制御部と、前記第１信号と前記第２信号を外部へ送信する送信部と、を備える装置により実現できる。

【００３４】

また、請求項２０に記載のように、前記制御部は、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化する構成とすることができる。

【００３５】

また、請求項２１に記載のように、前記制御部は、前記第２の換算定数を用い

て前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数及び前記第３の換算定数を用いて前記第２の代替値へ暗号化する構成とすることができる。

【００３６】

また、請求項２２に記載のように、前記制御部は、前記第２の換算定数及び前記第３の換算定数を用いて前記送信データを前記第１の代替値へ暗号化し、前記第１の換算定数を用いて前記第２の代替値へ暗号化する構成とすることができる。

【００３７】

また、請求項２３に記載のように、本発明は、第１の換算定数，第２の換算定数，第３の換算定数及び第４の換算定数のうち二の換算定数によって暗号化された送信データを送信する装置であって、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記第１の換算定数，前記第２の換算定数，前記第３の換算定数及び前記第４の換算定数を選択する換算定数選択処理と，前記第２の換算定数及び前記第４の換算定数を用いて前記送信データを第１の代替値に暗号化し前記第１の換算定数及び前記第３の換算定数を用いて前記送信データを第２の代替値へ暗号化する暗号化処理と，前記第１の代替値，前記第１の換算定数，及び前記第３の換算定数又は前記第４の換算定数に対応するパターン換算定数を含む第１信号を生成する第１信号生成処理と，前記第２の代替値，前記第２の換算定数，及び前記第１信号に含まれない前記第３の換算定数又は前記第４の換算定数のパターン換算定数を含む第２信号を生成する第２信号生成処理と，を行う制御部と、前記第１信号と前記第２信号を外部へ送信する送信部と、を備える装置により実現できる。

【００３８】

また、請求項２４に記載のように、本発明は、送信データの暗号化に用いられる換算定数に対応するパターン換算定数を含む信号を転送する装置であって、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記信号を送受信する送受信部と、受信した前記信号に含まれるパターン換算定数を対応する前記換算定数に変換して前記信号を変換する信号生成処理と，前記変換された信号を

転送する処理と，を行う制御部と、を備える装置により実現できる。

【００３９】

また、請求項２５に記載のように、本発明は、第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第１信号と第２´信号を受信して送信データを復号化する装置であって、前記第１信号には、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第１の代替値と，第１の換算定数と，が含まれ、前記第２´信号には、前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第２の代替値と，前記第２の換算定数と，前記第３の換算定数と，が含まれ、前記第１信号及び前記第２´信号を受信する受信部と、受信した前記第１信号から前記第１の代替値及び前記第１の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数及び前記第３の換算定数を読取る処理と，前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化処理と，前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２´信号を受け入れる認証をする認証処理と，を行う制御部と、を備える装置により実現できる。

【００４０】

また、請求項２６に記載のように、本発明は、第１の換算定数，第２の換算定数，第３の換算定数及び第４の換算定数のうち二の換算定数によって暗号化された送信データを含む第１´信号と第２´信号を受信して送信データを復号する装置であって、前記第１´信号には、前記第２の換算定数及び前記第４の換算定数を用いて前記送信データが暗号化された第１の代替値と，前記第１の換算定数と，前記第３の換算定数又は前記第４の換算定数と，が含まれ、前記第２´信号には、第１の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第１の代替値と，第２の換算定数と，前記第１´信号に含まれていない第３の換算定数又は前記第４の換算定数と，が含まれ、前記第１´信号及び前記第２´信号を受信する受信部と、受信した前記第１´信号から前記第１の代替値，前

記第１の換算定数，及び前記第３の換算定数又は第４の換算定数、前記第２´信号から前記第２の代替値，前記第２の換算定数，及び前記第３の換算定数又は第４の換算定数を読取る処理と，前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化処理と，前記第１の複合化データと前記第２の復号化データから前記第１´信号及び前記第２´信号を受け入れる認証をする認証処理と，を行う制御部を備える装置により実現できる。

【００４１】

また、請求項２７に記載のように、本発明は、第１の換算定数，第２の換算定数及び第３の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第１信号と第２信号を受信して送信データを復号化する装置であって、前記第１信号には、前記第２の換算定数，又は前記第２の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第１の代替値と，第１の換算定数と，が含まれ、前記第２信号には、前記第１の換算定数，又は前記第１の換算定数及び前記第３の換算定数を用いて前記送信データが暗号化された第２の代替値と，前記第２の換算定数と，前記第３の換算定数に対応するパターン換算定数と，が含まれ、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記第１信号及び前記第２信号を受信する受信部と、前記第１信号から前記第１の代替値，及び前記第１の換算定数、前記第２信号から前記第２の代替値，前記第２の換算定数，及び前記パターン換算定数を読取る処理と，前記読取られたパターン換算定数から前記第３の換算定数を取得する処理と，前記第１の代替値及び前記第２の代替値をそれぞれ暗号化に用いられた換算定数によって第１の復号化データ及び第２の復号化データへ復号化する復号化処理と，前記第１の複合化データと前記第２の復号化データから前記第１信号及び前記第２信号を受け入れる認証をする認証処理と，を行う制御部と、を備える装置により実現できる。

【００４２】

また、請求項２８に記載のように、前記制御部は、前記第１の復号化データ又は第２の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出するように構成することができる。

【００４３】

また、請求項２９に記載のように、前記制御部は、前記第１の複合化データと前記第２の復号化データが一致したときに前記認証を行うように構成することができる。

【００４４】

【発明の実施の形態】

本発明の実施の形態について図面を参照して説明する。図１は第１のデータ送信方法の説明図、図２は第２のデータ送信方法の説明図である。図３は実施例のデータ送信システムの説明図、図４は実施例のデータ送受信側装置の構成図、図５は実施例の送信データの暗号化についての説明図、図６は実施例の第１信号の構成を表す説明図、図７は実施例の第２信号の構成を表す説明図である。

【００４５】

図８は実施例の送信側装置のパターン換算定数データの説明図、図９は実施例の中継装置のパターン換算定数データの説明図、図１０は実施例の第２´信号の構成を表す説明図、図１１は実施例の送信信号の復号化についての説明図、図１２は実施例の送信信号の復号化についてのデータ例を示す説明図、図１３は実施例の送信側装置の処理の流れを示す説明図、図１４は実施例の中継装置の処理の流れを示す説明図、図１５及び図１６は実施例の受信側装置の処理の流れを示す説明図である。

【００４６】

図１７は第１のデータ送信方法の変形例を表す説明図、図１８は第１のデータ送信方法の変形例を表す説明図である。図１９は別実施例のデータ送信システムの説明図、図２０は別実施例のデータ送信システムの構成装置の構成図、図２１は別実施例の第１信号の構成を表す説明図、図２２は別実施例の第２信号の構成を表す説明図である。また、以下に説明する配置、形状等は、本発明を限定するものではなく、本発明の趣旨に沿って各種改変することができることは勿論である。

【００４７】

図１に基づき本発明のデータ送信システムに関する第１のデータ送信方法につ

いて説明する。本データ送信方法では、送信者（送信側装置）から受信者（受信側装置）へ、第１信号Ｓ１と第２信号Ｓ２が別々のルートで送信される。本発明の送信には、有線・無線回線を介した送信（例えば、赤外線通信，無線電波，光通信等による送信）及び伝送手段によるデータ等の送信（例えば、郵便等による配送）を含むものである。

【００４８】

まず、送信側装置では、暗号鍵となる換算定数Ｘ，Ｙとパターン換算定数Ｚが選択される。なお、送信側装置及び中継装置には、パターン換算定数Ｚに対して換算定数Ｚ´が関連付けて登録されている。送信側装置及び中継装置では、パターン換算定数Ｚが選択されると、これに対応して換算定数Ｚ´が読み出される。

【００４９】

送信側装置では、送信データＤは、換算定数ＹとＺ´の組合せによって暗号化データＤ（Ｙ，Ｚ´）に、換算定数ＸとＺ´の組合せによって暗号化データＤ（Ｘ，Ｚ´）に、それぞれ暗号化される。第１信号Ｓ１には、暗号化データＤ（Ｙ，Ｚ´），換算定数Ｘが含まれる。また、第２信号Ｓ２には、暗号化データＤ（Ｘ，Ｚ´），換算定数Ｙ，パターン換算定数Ｚが含まれる。

【００５０】

第１信号Ｓ１は、受信側装置へ送信される。一方、第２信号Ｓ２は、一旦、中継装置に送信される。そして、第２信号Ｓ２は、中継装置で第２´信号Ｓ２´に変換される。すなわち、中継装置では、受信された第２信号Ｓ２に含まれるパターン換算定数Ｚが換算定数Ｚ´に変換される。そして、第２´信号Ｓ２´は、中継装置から受信側装置へ送信される。なお、第１信号Ｓ１及び第２信号Ｓ２は、送信側装置から時間をずらして送信されるようにしてもよい。

【００５１】

受信側装置では、第１信号Ｓ１及び第２´信号Ｓ２´を受信し、第１信号Ｓ１から換算定数Ｘ、第２´信号Ｓ２´から換算定数Ｙ，Ｚ´が読取られる。そして、第１信号Ｓ１に含まれる暗号化データＤ（Ｙ，Ｚ´）は、読取られた換算定数ＹとＺ´の組合せによって復号化され、復号化データＤ１が算出される。一方、第２´信号Ｓ２´に含まれる暗号化データＤ（Ｘ，Ｚ´）は、読取られた換算定

数ＸとＺ´の組合せによって復号化され、復号化データＤ２が算出される。

【００５２】

そして、復号化データＤ１とＤ２との比較が行われる。受信側では両者が一致した場合に、復号化データＤ１（又はＤ２）を送信データＤとして採用する。また、送信データＤには、受信側装置に接続された種々の外部駆動装置を駆動させるための駆動信号を含ませることができる。例えば、外部駆動装置としてのロックシステムを開閉操作することが可能となる。

【００５３】

なお、上記暗号化例では、送信データＤを換算定数ＹとＺ´の組合せ及び換算定数Ｘ，Ｚ´の組合せにより暗号化していたが、これに限らず、送信データＤを換算定数ＹとＺ´の組合せによる暗号化（Ｄ（Ｙ，Ｚ´））及び換算定数Ｘのみによる暗号化（Ｄ（Ｘ））をするようにしてもよい。この場合、第１信号Ｓ１には暗号化データＤ（Ｙ，Ｚ´），換算定数Ｘが含まれ、第２信号Ｓ２には暗号化データＤ（Ｘ），換算定数Ｙ，パターン換算定数Ｚが含まれる。

【００５４】

また、送信データＤを換算定数Ｙのみによる暗号化（Ｄ（Ｙ）），換算定数ＸとＺ´による暗号化（Ｄ（Ｘ，Ｚ´））をするようにし、第１信号Ｓ１には暗号化データＤ（Ｙ），換算定数Ｘが含まれ、第２信号Ｓ２には暗号化データＤ（Ｘ，Ｚ´），換算定数Ｙ，パターン換算定数Ｚが含まれるようにすることもできる。

【００５５】

このようにすれば、成りすまし送信された場合に、中継装置では不正な第２信号Ｓ２に含まれるパターン換算定数Ｚが、登録された対応関係により換算定数Ｚ´に変換される。そして、この対応関係が正しくない換算定数Ｚ´を含む第２´信号Ｓ２´が受信側へ転送される。

【００５６】

しかし、この換算定数Ｚ´は成りすまし送信での暗号化に使用された換算定数とは異なるため、受信側で不正な第１信号Ｓ１と不正な第２´信号Ｓ２´をもとに復号化すると、得られる復号化データＤ１とＤ２が不一致となる。また、復号

化データは、有意なデータとして復号することはできない。

【００５７】

以上のように第１のデータ送信方法では暗号化された送信データを２系統で送信する場合に、第１信号Ｓ１に含まれる暗号化データの暗号鍵（換算定数Ｙ）は第２信号Ｓ２に含めて送信され、第２信号Ｓ２に含まれる暗号化データの暗号鍵（換算定数Ｘ）は第１信号Ｓ１に含めて送信される。

【００５８】

さらに、第１信号Ｓ１及び第２信号Ｓ２に含まれる暗号化データの共通の暗号鍵（換算定数Ｚ´）そのものは送付されず、暗号鍵に対応するパターン換算定数Ｚが第２信号Ｓ２に含めて中継装置へ送信される。そして、このパターン換算定数Ｚが、中継装置で換算定数Ｚ´へ変換されることにより、第２信号Ｓ２が第２´信号Ｓ２´に変換され、受信側へ転送される。

【００５９】

このように送信することにより、第３者は第１信号Ｓ１及び第２信号Ｓ２の双方を取得したとしてもパターン換算定数Ｚが不明であるので、送信データＤの復号化を行うことはできない。また、第３者が第１信号Ｓ１又は第２´信号Ｓ２´の一方を取得したとしても、それぞれの信号には換算定数のすべての換算定数が含まれていないので、復号化を行うことはできない。

【００６０】

さらに、第３者が第１信号Ｓ１及び第２´信号Ｓ２´の双方を取得したとしても、復号化方法を取得しない限り、有意な復号化データを得ることはできない。

【００６１】

以上のように、第１のデータ送信方法では、第３者が暗号化データを不正に取得したとしても、暗号化データの復号化を有意に行うことができず、送信データの秘匿性を高めることができる。

【００６２】

また、受信側では、送信側で登録されたパターン換算定数を知らなくても暗号化データを復号化することができる。したがって、送信側では複数のパターン換算定数Ｚ及び換算定数Ｚ´の組合せを登録することにより、複数の受信者（受信

側装置）へ暗号化データを送信する場合にも秘匿性を高めることができる。

【００６３】

そして、第３者には換算定数Ｘ，Ｙ，Ｚ´による暗号化方法及びパターン換算定数が不明であるため、送信者に成り代わって送信したとしても、受信側では有意なデータとして復号化することができない。または、復号化データが一致しない。これにより、成りすまし送信による不都合を回避することができる。

【００６４】

次に、図２に基づき第２のデータ送信方法について説明する。送信者（送信側装置）から受信者（受信側装置）へ第１信号S_1と第２信号S_2が別々のルートで送信されるのは、第１のデータ送信方法と同様である。また、送信側装置から送信される第１信号S_1及び第２信号S_2についても、暗号化方法やそれぞれに含められる換算定数等は同様である。

【００６５】

第２のデータ送信方法と上述の第１のデータ送信方法との違いは、第２信号S_2が中継装置を介して送信されないことである。そのため、第１のデータ送信方法では送信側と中継装置にパターン換算定数Ｚ及び換算定数Ｚ´が登録されていたが、第２のデータ送信方法では送信側と受信側にパターン換算定数Ｚ及び換算定数Ｚ´が登録されている。

【００６６】

したがって、受信側装置では、第１信号S_1及び第２信号S_2が受信され、第１信号S_1から換算定数Ｘ、第２信号S_2から換算定数Ｙ及びパターン換算定数Ｚが読取られる。そして、受信側装置で読取られたパターン換算定数Ｚに対応する換算定数Ｚ´が読み込まれる。

【００６７】

これにより、第１信号S_1に含まれる暗号化データＤ（Ｙ，Ｚ´）（又はＤ（Ｙ））は、換算定数ＹとＺ´の組合せ（又はＹのみ）によって復号化データD_1に復号化され、第２信号S_2に含まれる暗号化データＤ（Ｘ，Ｚ´）（又はＤ（Ｘ））は、換算定数ＸとＺ´の組合せ（又はＸのみ）によって復号化データD_2に復号化される。

【００６８】

または、第１信号Ｓ１に含まれる暗号化データＤ（Ｙ，Ｚ´）（又はＤ（Ｙ））は、換算定数ＹとＺ´の組合せ（又はＹ）によって復号化データＤ１に復号化され、第２信号Ｓ２に含まれる暗号化データＤ（Ｘ）（又はＤ（Ｘ，Ｚ´））は、換算定数Ｘ（又はＸとＺ´の組合せ）によって復号化データＤ２に復号化される。

【００６９】

そして、受信側では第１のデータ送信方法と同様に両者が一致した場合に、復号化データＤ１（又はＤ２）が送信データＤとして採用される。

【００７０】

以上のように第２のデータ送信方法では暗号化された送信データを２系統で送信する場合に、第１信号Ｓ１に含まれる暗号化データの暗号鍵（換算定数Ｙ）は第２信号Ｓ２に含めて送信され、第２信号Ｓ２に含まれる暗号化データの暗号鍵（換算定数Ｘ）は第１信号Ｓ１に含めて送信される。これは、第１のデータ送信方法と同様である。

【００７１】

そして、第１信号Ｓ１及び第２信号Ｓ２に含まれる暗号化データの共通の暗号鍵（換算定数Ｚ´）そのものは送付されず、暗号鍵に対応するパターン換算定数Ｚが第２信号Ｓ２に含めて送信される。

【００７２】

そして、第２信号Ｓ２を受信した受信側装置では、予め有しているパターン換算定数Ｚと換算定数Ｚ´の組合せの登録データを参照して、第２信号Ｓ２に含まれるパターン換算定数Ｚから換算定数Ｚ´を読み込み、さらに第１信号Ｓ１及び第２信号Ｓ２から得られた換算定数Ｘ，Ｙを使用して、送信データＤを復号化している。

【００７３】

このように、送信側及び受信側に予めパターン換算定数を登録しておくことにより、送信側と受信側との一対一の秘匿データ送信が可能となる。このような、送信方法を利用して、例えば外部駆動装置としてのドアロックの開閉操作等を行

うことができる。漏洩データに対する復号化が困難であること、及び成りすまし送信による不都合を回避できることは、第１のデータ送信方法と同様である。

【００７４】

なお、第１及び第２の送信方法では、換算定数Ｘ，Ｙ，Ｚの３つの暗号鍵を用いて暗号化しているが、換算定数Ｘ，Ｙ，Ｚは、それぞれ換算定数$Ｘ_1$，$Ｘ_2$，・・・、換算定数$Ｙ_1$，$Ｙ_2$，・・・、換算定数$Ｚ_1$，$Ｚ_2$，・・・、のようにそれぞれ複数の換算定数を含む概念である。また、例えば、換算定数Ｘに複数の換算定数（$Ｘ_1$，$Ｘ_2$，・・・）が用いられる場合は、これら複数の換算定数を第１信号$Ｓ_1$，第２信号$Ｓ_2$のどちらか、もしくは分散して両方に配置してもよい。

【００７５】

次に、第１の送信方法を用いた実施例の概略を図３に基づいて説明する。本例のデータ送信システムＳは、一方の送受信装置１（以下、「装置１」という）からインターネットＩを介して他方の送受信装置１へ暗号化された送信データを送信するものである。

【００７６】

第１信号$Ｓ_1$は、送信側の装置１からプロバイダＰを介して受信側の装置１のアドレスへ向けて送信され、受信側の装置１は第１信号$Ｓ_1$を受信する。また、第２信号$Ｓ_2$は、送信側の装置１からプロバイダＰを介して中継配信サーバプロバイダ２（以下、「中継装置２」という）へ向けて送信される。中継装置２では、第２信号$Ｓ_2$を第２´信号$Ｓ_2$´に変換して、これを受信側の装置１のアドレスへ向けて送信する。受信側の装置１は、第２´信号$Ｓ_2$´を受信する。

【００７７】

本例のデータ送信システムＳでは、送信データとして個人認証番号Ａ，搬送認証番号Ｂ，制御データＣ，機密データＤｔが送信される。個人認証番号Ａ，搬送認証番号Ｂ，制御データＣは、第１乃至第３の換算定数としての換算定数Ｘ，Ｙ，Ｚｙ´で暗号化され、第１信号$Ｓ_1$及び第２信号$Ｓ_2$に含められる。また、機密データＤｔは別途秘匿化されて第１信号$Ｓ_1$に含められる。

【００７８】

受信側の装置１では、第１信号Ｓ１及び第２´信号Ｓ２´を受信して、両信号から換算定数Ｘ，Ｙ，Ｚｙ´を読取り、これらにより両信号に含まれる暗号化された個人認証番号Ａ，搬送認証番号Ｂ，制御データＣに関するデータを復号し、また、機密データＤｔの復号化を行う。さらに、復号化された制御データＣに基づき、外部装置が駆動される。

【００７９】

本例の換算定数Ｘ，Ｙは、乱数によって装置１内で生成される。したがって、送信毎に異なる換算定数が選択されるものである。また、送信側の装置１は、特有のパターン換算定数データを有しており、パターン換算定数データには、パターン換算定数Ｚｙと換算定数Ｚｙ´の複数の組合せ（本例では、２６通り）が送信者により登録されている。なお、このパターン換算定数データは、中継装置２にも送信者毎に対応して登録されている。

【００８０】

本システムＳに登録された送信者は、固有の個人認証番号Ａを有しており、装置１を用いて個人認証番号Ａ，搬送認証番号Ｂ，制御データＣ，機密データＤｔを送信することができる。受信者は、送信者から送られてきた２つの信号を受信し、これらから装置１によって送信データの認証を行い、個人認証番号Ａ，搬送認証番号Ｂ，制御データＣ，機密データＤｔを取得することができる。

【００８１】

搬送認証番号Ｂは、送信者が商品の搬送認証番号等を受信者に送付するためのものであり、売り手側から買い手側へ商品等を受け渡す流通手段として、又は受け渡しロッカー等の用途に使用することができる。また、クレジットカード番号の送信にも使用することができる。

【００８２】

制御データＣは、送信側から受信側へ販売金額，利用回数，バーコード出力，リモート制御のＯＮ／ＯＦＦ信号，鍵の解錠／施錠信号等の制御信号を送付するためのものである。

【００８３】

機密データＤｔは、送信者が受信者へ見積書，医療カルテ，法文書，成績書そ

の他の機密文書等を封印して送信するためのものである。機密データＤｔは別途秘匿化されて第１信号Ｓ$_1$に含められる。

【００８４】

中継装置２には、上述のように複数の登録送信者ごとのパターン換算定数データが記憶されており、各登録送信者からの第２信号Ｓ$_2$を受信して、該信号中のパターン換算定数を該当する換算定数へ変換して第２´信号Ｓ$_2$´を生成し、第２信号Ｓ$_2$に付随して送信されてきた受信者のアドレスへ転送している。

【００８５】

また、中継装置２は、このようなデータ管理，データ変換及びデータ転送等の処理を行うと共に、データ転送等の処理に基づいて課金を行うための課金データ作成処理を行う。これにより、各登録送信者に対して、利用に応じて利用料の請求を行うことができる。このような課金については、利用回数、データ量等に応じて行うことが考えられる。

【００８６】

次に、図４に基づいて装置１及び中継装置２の構成について説明する。装置１は、専用機として構成してもよいが、通常のデスクトップ型のパソコンやモバイル端末を使用した構成としてもよい。装置１は、制御部としてのＣＰＵ１００と、データの入出力を行うための入出力部１０１と、データの表示を行うための表示部１０２と、送受信部１０３と、各種データが記憶された記憶部１１０と、を備えている。

【００８７】

ＣＰＵ１００は、データの入出力制御、データ送受信制御、データの暗号化及び復号化処理、データ読取処理，第１信号及び第２信号の生成処理、認証処理、外部駆動装置の制御等を行う。データの暗号化処理については、ＣＰＵ１００は、乱数によって換算定数を自動選択（換算定数選択処理）し、該換算定数による所定の暗号化式にしたがって暗号化手段として入力データの暗号化（暗号化処理）を行う。なお、換算定数は送信者が指定して、該換算定数がＣＰＵ１００に選択されるようにしてもよい。

【００８８】

入出力部１０１は、送信データとしての個人認証番号Ａ，搬送認証番号Ｂ等や受信者のアドレス入力、パターン換算定数データ登録、データ暗号化・復号化処理，バーコードの読取処理等に用いられるものであり、例えばキーボード，マウス，バーコードリーダー，各種記憶メディアとのデータ入出力装置等から構成される。

【００８９】

表示部１０２は、入出力データ等の表示を行うものであり、例えばＬＣＤ装置等から構成される。送受信部１０３は、インターネットＩ及び外部駆動装置等に接続され、外部とデータの送受信を行うものであり、例えばモデムやＬＡＮカード等である。

【００９０】

記憶部１１０は、主記憶部１１１と、ＲＯＭ１１２と、ＲＡＭ１１３とを備える。主記憶部１１１には、オペレーティングシステムプログラムや、本例のデータ送受信処理等を行うためのプログラムを含む各種アプリケーションプログラム、パターン換算定数データ１１１ａ等が記憶されている。また、ＲＯＭ１１２には、基本プログラム等が記憶され、ＲＯＭ１１３は作業エリアとして用いられる。

【００９１】

送信者は、データ送信時にデータ送信システムＳ用の制御プログラムを起動して装置１の入出力部１０１から所定のデータの入力操作及びその他の送信操作を行う。また、受信者は、信号を受信して復号操作等を行う。

【００９２】

また、本例の中継装置２は、プロバイダ内に配設されるサーバコンピュータとして実現することができる。中継装置２は、制御部としてのＣＰＵ２００、入出力部２０１、表示部２０２、送受信部２０３、記憶部２１０とを備えている。記憶部２１０は、主記憶部２１１、ＲＯＭ２１２、ＲＡＭ２１３を備えている。また、主記憶部２１１内には、上述した登録者毎のパターン換算定数データ２１１ａが記憶されている。ＣＰＵ２００は、信号の送受信処理、データ読取処理，信号の変換処理（信号生成処理）等を行う。

【００９３】

次に、図５に基づき送信データの暗号化について説明する。上述のように本例の暗号化には乱数によって生成される換算定数Ｘ，Ｙ、及び送信者が選択するパターン換算定数Ｚｙに対応する換算定数Ｚｙ´が用いられる。なお、パターン換算定数Ｚｙは送信者が選択するのではなく、暗号化時に登録されたパターン換算定数データから自動的に選択されるように構成してもよい。

【００９４】

図５に示すように、個人認証番号Ａは第１式（Ａｘ＝Ａ＋Ｙ＋Ｚｙ´）及び第２式（Ａｙ＝Ａ＋Ｘ＋Ｚｙ´）、搬送認証番号Ｂは第１式（Ｂｘ＝Ｂ＋Ｙ＋Ｚｙ´）及び第２式（Ｂｙ＝Ｂ＋Ｘ＋Ｚｙ´）、制御データＣは第１式（Ｃｘ＝Ｃ＋Ｙ＋Ｚｙ´）及び第２式（Ｃｙ＝Ｃ＋Ｘ＋Ｚｙ´）にしたがい暗号化される。それぞれのデータは、個人ＩＤ代替値（Ａｘ，Ａｙ），搬送ＩＤ代替値（Ｂｘ，Ｂｙ），制御データ代替値（Ｃｘ，Ｃｙ）に暗号化される。

【００９５】

例えば、図５に示したように、個人認証番号Ａを「１２３４５６７８９０１２」，搬送認証番号Ｂを「０３１２３４５６７８９０」，制御データＣを「２００００」，換算定数Ｘを「２２３３４４」，換算定数Ｙを「４４５５６６」，換算定数Ｚを「３３９９」とすると、それぞれのデータは第１式及び第２式によって、個人認証番号Ａは「１２３４５７２３７９７７」，「１２３４５７０１５７５５」、搬送認証番号Ｂは「０３１２３５０１６８５５」，「０３１２３４７９４６３３」、制御データＣは「４６８９６５」，「２４６７４３」に暗号化される。

【００９６】

本例の暗号化は、図５に示したように送信データに換算定数ＸとＺｙ´，換算定数ＹとＺｙ´がそれぞれ加算されるものであるが、これに限らず、減算，その他の演算方法であってもよい。また、上述したように送信データに換算定数ＸとＺ´，換算定数Ｙのみによって演算する方法、又は、送信データに換算定数Ｘのみ，換算定数ＹとＺ´によって演算する方法により暗号化してもよい。

【００９７】

例えば、送信データに換算定数Ｘのみ，換算定数ＹとＺ´による加算を行う場合は、個人認証番号Ａは第１式（Ａｘ＝Ａ＋Ｙ＋Ｚｙ´）及び第２式（Ａｙ＝Ａ＋Ｘ）、搬送認証番号Ｂは第１式（Ｂｘ＝Ｂ＋Ｙ＋Ｚｙ´）及び第２式（Ｂｙ＝Ｂ＋Ｘ）、制御データＣは第１式（Ｃｘ＝Ｃ＋Ｙ＋Ｚｙ´）及び第２式（Ｃｙ＝Ｃ＋Ｘ）にしたがい暗号化される。このようにすると、より成りすまし送信に対する不都合を排除する効果を向上させることができる。

【００９８】

次に、図６及び図７に基づき第１信号$Ｓ_1$及び第２信号$Ｓ_2$について説明する。第１信号$Ｓ_1$及び第２信号$Ｓ_2$は、それぞれ大きさが指定されたパケット１乃至パケット１０の１０のデータ領域からなる。パケット０は、第１信号$Ｓ_1$及び第２信号$Ｓ_2$の内容を作成する際に入力するパスワードを一時的に格納するための領域であって、実際にデータとしては送信されないものである。

【００９９】

パケット１は、通信番号格納領域であって送信信号に対して自動的に生起される番号である。パケット２は、送信者アドレス格納領域であって送信者の電子メールアドレスが入力される。パケット３は、送信者の登録名の格納領域である。

【０１００】

パケット４は、第１信号$Ｓ_1$の場合は換算定数Ｘが、第２信号$Ｓ_2$の場合は換算定数Ｙが格納される領域である。パケット５は、パターン換算定数Ｚｙの格納領域である。本例の場合、パターン換算定数Ｚｙは第１信号$Ｓ_1$には入力されず、第２信号$Ｓ_2$のみに入力される。図７の例では、パターン換算定数Ｚｙとして「ｇ」が選択されている。パターン換算定数Ｚｙの「ｇ」は、換算定数Ｚの「３９９」に対応している。

【０１０１】

パケット６は、第１信号$Ｓ_1$，第２信号$Ｓ_2$において、個人認証番号Ａがそれぞれ第１式，第２式によって暗号化された個人ＩＤ代替値Ａｘ，Ａｙが格納される領域である。同様にパケット７は、搬送認証番号Ｂがそれぞれ第１式，第２式によって暗号化された搬送ＩＤ代替値Ｂｘ，Ｂｙが格納される領域である。また、パケット８は、制御データＣがそれぞれ第１式，第２式によって暗号化された

制御データ代替値Ｃｘ，Ｃｙが格納される領域である。

【０１０２】

パケット９は、制御パターンＣｐが格納される領域である。制御パターンＣｐとは、制御データＣの制御パターンを指定するものであり、例えば制御パターンＣｐがａの場合は、制御データＣは回数を意味するものであることを表す。

【０１０３】

同様に制御パターンＣｐが、ｂ，ｃ，ｄ，ｅのときは、それぞれ制御データＣは、プリペイド金額・販売金額等の金額データ，数値・バーコード出力等の数値データ，リモート制御のためのＯＮ／ＯＦＦ信号データ，ロックシステムの解錠／施錠信号データを意味するものであることを表す。本例の場合、制御パターンＣｐは第１信号Ｓ１のみに格納される。図６の例では、制御パターンＣｐとして「ｂ」が選択されている。

【０１０４】

また、パケット１０は、機密データＤｔが格納される領域である。本例の場合、機密データＤｔは第１信号Ｓ１のみに格納される。以上のような第１信号Ｓ１及び第２信号Ｓ２は、電子メールに添付されるデータファイルの形式で送信することができる。なお、制御パターンＣｐ，機密データＤｔは、第２信号Ｓ２に配置されてもよい。

【０１０５】

図８に示すように、装置１内に記憶されるパターン換算定数データ１１１ａは、パターン換算定数Ｚ（ａ，ｂ，・・・）にそれぞれ対応して換算定数Ｚｙ´（１２３４，２３４５，・・・）が関係付けられたものである。登録送信者は、装置１に自らが指定した２６の換算定数Ｚｙ´を登録することができる。また、データ送信システムＳの管理者を介して、又は、直接、中継装置２に自ら指定したパターン換算定数データ１１１ａを登録することができる。

【０１０６】

図９に示すように、中継装置２内に登録されるパターン換算定数データ２１１ａは、複数の登録送信者のパターン換算定数データ１１１ａから構成されている。登録送信者ごとのパターン換算定数データ１１１ａは、各登録送信者の電子メ

ールアドレス及び送信者の登録名によって区別されている。

【０１０７】

次に、図１０に基づき第２´信号Ｓ２´について説明する。送信側の装置１からの第２信号Ｓ２は、プロバイダＰ経由で中継装置２へ一旦送信される。中継装置２では、上述のように第２信号Ｓ２から第２´信号Ｓ２´に変換される。

【０１０８】

中継装置２では、第２信号Ｓ２のパケット２（送信者アドレス）及びパケット３（登録名）を参照して、パターン換算定数データ２１１ａから送信者のパターン換算定数データ１１１ａが選択される。そして、選択されたパターン換算定数データ１１１ａから第２信号Ｓ２のパケット５（パターン換算定数Ｚｙ）を参照して、これに対応する換算定数Ｚｙ´が特定される。

【０１０９】

換算定数Ｚｙ´が特定されると、第２信号Ｓ２のパケット５が、特定されたパターン換算定数Ｚｙ´の値に変換された第２´信号Ｓ２´が生成される。このように、中継装置２では、受信された第２信号Ｓ２が第２´信号Ｓ２´に変換される。そして、第２´信号Ｓ２´は、送信者が指定する受信者の電子メールアドレスへ転送される。図１０の例では、第２´信号Ｓ２´のパケット５（パターン換算定数格納領域）は「ｇ」から「３３９９」へ変換される。

【０１１０】

次に、図１１に基づき受信側の装置１で行われる復号化処理の概略について説明する。受信側の装置１で第１信号Ｓ１及び第２´信号Ｓ２´が受信されると、両信号がペアリングされて仮認証される。このとき、通信番号，発信者アドレス等の一致が確認される。仮認証の結果、両信号が同一送信者からの受信信号であることが確認されると、両信号の暗号化データの復号化処理が行われる。

【０１１１】

まず、復号化処理では、両信号から換算定数Ｘ，Ｙ，Ｚｙ´が特定される。次に、個人ＩＤ代替値を復号化するための第１式（Ａ１＝Ａｘ－Ｙ－Ｚｙ´）及び第２式（Ａ２＝Ａｙ－Ｙ－Ｚｙ´）によってそれぞれ第１信号Ｓ１の個人ＩＤ代替値Ａｘ，第２´信号Ｓ２´の個人ＩＤ代替値Ａｙが復号化される。

【０１１２】

そして、第１信号Ｓ１及び第２´信号Ｓ２´のパケット３の送信者の登録名が一致すること、及び、復号化されたデータ（Ａ１，Ａ２）が一致することが確認される。登録名及び復号化データＡ１とＡ２が一致すれば、両信号が最終的に認証される。

【０１１３】

なお、個人ＩＤ代替値を復号化するための第１式がＡ１＝Ａｘ－Ｙ－Ｚｙ´であり、第２式がＡ２＝Ａｙ－Ｙである場合も同様に個人ＩＤ代替値Ａｘ，Ａｙが復号化されて復号化データＡ１及びＡ２が算出され、登録名及び復号化データＡ１及びＡ２の比較が行われ、両者が一致すれば、両信号が最終的に認証される。

【０１１４】

また、最終的に認証されると、搬送ＩＤ代替値を復号化するための第１式（Ｂ１＝Ｂｘ－Ｙ－Ｚｙ´）及び第２式（Ｂ２＝Ｂｙ－Ｙ－Ｚｙ´）によってそれぞれ第１信号Ｓ１の搬送ＩＤ代替値Ｂｘ，第２´信号Ｓ２´の搬送ＩＤ代替値Ｂｙが復号化され、復号化データＢ１とＢ２が一致すれば、搬送認証番号Ｂとして復号化データＢ１（又はＢ２）が採用される。

【０１１５】

また、同様に、制御データ代替値を復号化するための第１式（Ｃ１＝Ｃｘ－Ｙ－Ｚｙ´）及び第２式（Ｃ２＝Ｃｙ－Ｙ－Ｚｙ´）によってそれぞれ第１信号Ｓ１の制御データ代替値Ｃｘ，第２´信号Ｓ２´の制御データ代替値Ｃｙが復号化され、復号化データＣ１とＣ２が一致すれば、制御データＣとして復号化データＣ１（又はＣ２）が採用される。

【０１１６】

搬送ＩＤ代替値を復号化するための第１式がＢ１＝Ｂｘ－Ｙ－Ｚｙ´、第２式がＢ２＝Ｂｙ－Ｙであり、制御データ代替値を復号化するための第１式がＣ１＝Ｃｘ－Ｙ－Ｚｙ´、第２式がＣ２＝Ｃｙ－Ｙ－Ｚｙ´である場合も同様である。

【０１１７】

また、制御パターンＣｐにより、制御データＣの種類が特定される。さらに、制御データＣの種類が、外部駆動装置へのＯＮ／ＯＦＦ信号データ、解錠／施錠

信号データであった場合は、受信側の装置１からさらに外部装置へ該信号が送出され、外部駆動装置が駆動されるようになっている。

【０１１８】

図１２に示すように、両信号の登録名が「ｘｘｘｘｘｘ」であるので、登録名（Ｎｍ）は一致する。そして、個人ＩＤ代替値Ａｘとして「１２３４５７２３７９７７」，個人ＩＤ代替値Ａｙとして「１２３４５７０１５７５５」を受信していた場合、換算定数Ｘ，Ｙ，Ｚｙ′を所定のパケットから読み出して復号化が行われると、図１２の場合、復号化データ$Ａ_1$及び$Ａ_2$は共に「１２３４５６７８９０１２」となり両者は一致するため、両信号は正規のものであるとの最終認証が行われる。

【０１１９】

また、搬送ＩＤ代替値Ｂｘ，Ｂｙがそれぞれ「０３１２３５０１６８５５」，「０３１２３４７９４６３３」であった場合は、復号化データ$Ｂ_1$と$Ｂ_2$が共に「０３１２３４５６７８９０」となるので両者は一致する。

【０１２０】

また、制御データ代替値Ｃｘ，Ｃｙがそれぞれ「４６８９６５」，「２４６７４３」であった場合は、復号化データ$Ｃ_1$と$Ｃ_2$が共に「２００００」となるので両者は一致する。これにより、搬送認証番号Ｂ，制御データＣには、それぞれ「０３１２３４５６７８９０」，「２００００」が採用される。

【０１２１】

次に、図１３に基づき送信側の装置１のデータ処理の流れについて説明する。まず、ステップＳ１０では、画面表示に従って送信者が入力した所定のデータが読み込まれる。所定の入力データとしては、第１信号$Ｓ_1$及び第２信号$Ｓ_2$に関連したものとして、送信者の電子メールアドレス（パケット２），送信者名（登録名、パケット３），パターン換算定数Ｚｙ（パケット５），個人認証番号Ａ，搬送認証番号Ｂ，制御データＣ，制御パターンＣｐ（パケット９），機密データＤｔ、また、他のデータとして受信者の電子メールアドレス，中継装置２の電子メールアドレス等がある。

【０１２２】

なお、パスワード（パケット０）を入力するようにして、登録送信者以外の者が装置１を用いて送信操作できないように制限をかけるようにしてもよい。

【０１２３】

次にステップＳ１１では、データ入力（Ｓ１０）されたタイミングで選択された２つの乱数（本例の場合６桁の数）を換算定数Ｘ，Ｙとし、また、ステップＳ１０で入力されたパターン換算定数Ｚｙに対応する換算定数Ｚｙ´をパターン換算定数データ１１１ａから読み出す。

【０１２４】

そして、ステップＳ１２へ進み、ステップＳ１０で入力された個人認証番号Ａ，搬送認証番号Ｂ，制御データＣを換算定数Ｘ，Ｙ，Ｚｙ´によって暗号化し、また、別途機密データＤｔを暗号化する。機密データＤｔの暗号化手法については、個人認証番号Ａ，制御データＣや換算定数Ｚｙ´等を暗号鍵として暗号化してもよい。

【０１２５】

ステップＳ１３では、ステップＳ１２で暗号化されたデータ及びステップＳ１０で入力された入力データに基づき、所定の大きさを有する格納領域に各データを配置することにより第１信号$Ｓ_1$が生成される。

【０１２６】

次にステップＳ１４では、ステップＳ１３と同様に第２信号$Ｓ_2$が生成される。ステップＳ１３及びＳ１４では、例えば第１信号$Ｓ_1$のパケット５のように配置すべきデータがない場合には、ブランクデータもしくは所定のスクランブルデータが配置される。

【０１２７】

また、例えば搬送認証番号Ｂは送信するが、制御データＣは送信する必要がない場合、制御データＣにはステップＳ１０でブランクデータが入力される。この場合も、ブランクデータ（又はスクランブルデータ）を入力データとして、ステップＳ１３及びＳ１４でデータが生成される。

【０１２８】

そして、ステップＳ１５では、送信者の送信入力に基づいて、先ず指定された

受信者のアドレスへ第１信号Ｓ１が送信される。次いでステップＳ１６で、指定された中継装置２のアドレスへ第２信号Ｓ２が送信され、処理を終了する。

【０１２９】

次に、図１４に基づき中継装置２での処理の流れについて説明する。中継装置２は、ステップＳ２０で所定の電子メールアドレスに送信者からの第２信号Ｓ２が送信されてくるのを待ち、ステップＳ２０で第２信号Ｓ２を受信すると（ステップＳ２０；Ｙｅｓ）、ステップＳ２１へ進み、送信者の識別を行う。

【０１３０】

ステップＳ２１では、受信した第２信号Ｓ２の送信者の電子メールアドレス（パケット２）及び登録名（パケット３）を読み込む。そして、ステップＳ２２で、該電子メールアドレス及び登録名がパターン換算定数データ２１１ａに登録されているか否かを判別する。

【０１３１】

ステップＳ２２で該電子メールアドレス及び登録名が登録されていれば（ステップＳ２２；Ｙｅｓ）、パターン換算定数データ１１１ａを特定してステップＳ２３へ進む。一方、登録されていなければ（ステップＳ２２；Ｎｏ）、正規の登録送信者からの信号でないと判断して処理を終了する。なお、このとき、受信者へ不正な第２信号Ｓ２を受信した旨の電子メールを送信するようにしてもよい。

【０１３２】

ステップ２３では、第２信号Ｓ２のパターン換算定数Ｚｙ（パケット５）を読取る。ステップＳ２４では、ステップＳ２２で特定されたパターン換算定数データ１１１ａを参照して、読取られたパターン換算定数Ｚｙに対応する換算定数Ｚｙ´を読取る。

【０１３３】

そして、ステップＳ２５で、ステップＳ２４で読取られた換算定数Ｚｙ´を用いて第２´信号Ｓ２´を生成する。ステップＳ２６では、ステップＳ２５で生成された第２´信号Ｓ２´を、第２信号Ｓ２と共に送付されてきた受信者の電子メールアドレスに送信し、処理を終了する。

【０１３４】

次に、図１５及び図１６に基づき、受信側の装置１の処理の流れについて説明する。ステップＳ３０で、第１信号$Ｓ_1$及び第２´信号$Ｓ_2$´を受信して装置１内に取り込む。そして、装置１に取り込まれた第１信号$Ｓ_1$及び第２´信号$Ｓ_2$´が受信者によって一対の信号であると指定される。具体的には、受信者が受取った電子メールに添付されたデータファイルが、装置１の画面上で第１信号$Ｓ_1$及び第２´信号$Ｓ_2$´に指定される。

【０１３５】

ステップＳ３２では、指定された２つの信号の通信番号（パケット１）に相当するデータが比較される。両信号の通信番号が一致した場合は（ステップＳ３２；Ｙｅｓ）、ステップＳ３３へ進む。一方、両信号の通信番号が一致しなかった場合は（ステップＳ３２；Ｎｏ）、ステップＳ４８へ進み、表示部１０２にその旨のエラー表示をして処理を終了する。

【０１３６】

ステップＳ３３では、第１信号$Ｓ_1$のパケット３乃至パケット１０のデータが読取られる。また、ステップＳ３４では、第２´信号$Ｓ_2$´のパケット３乃至パケット１０のデータが読取られる。

【０１３７】

次にステップＳ３５では、個人ＩＤ代替値Ａｘを復号化するための第１式から復号化データ$Ａ_1$が算出される。ステップＳ３６では、個人ＩＤ代替値Ａｙを復号化するための第２式から復号化データ$Ａ_2$が算出される。そして、ステップＳ３７でステップＳ３３及びＳ３４で読取られた登録名、復号化データ$Ａ_1$と$Ａ_2$がそれぞれ比較され、一致するか否かが判別される。

【０１３８】

これらが一致すると（ステップＳ３７；Ｙｅｓ）、ステップＳ３８へ進む。一方、一致しなかった場合は（ステップＳ３７；Ｎｏ）、ステップＳ４９へ進み、登録名，復号化データ$Ａ_1$と$Ａ_2$が一致しない旨のエラー表示をして処理を終了する。一致しない場合としては、成りすまし送信で暗号化式が不正であった場合、成りすまし送信でパターン換算定数Ｚｙと換算定数Ｚｙ´との対応関係の不一致の場合等である。

【０１３９】

ステップＳ３８では、搬送ＩＤ代替値Ｂｘを復号化するための第１式から復号化データＢ$_1$が算出される。ステップＳ３９では、搬送ＩＤ代替値Ｂｙを復号化するための第２式から復号化データＢ$_2$が算出される。そして、ステップＳ４０で復号化データＢ$_1$とＢ$_2$が比較され、一致するか否かが判別される。

【０１４０】

これらが一致すると（ステップＳ４０；Ｙｅｓ）、ステップＳ４１へ進む。一方、一致しなかった場合は（ステップＳ４０；Ｎｏ）、ステップＳ５０へ進み、復号化データＢ$_1$とＢ$_2$が一致しない旨のエラー表示をして処理を終了する。

【０１４１】

ステップＳ４１では、制御データ代替値Ｃｘを復号化するための第１式から復号化データＣ$_1$が算出される。ステップＳ４２では、制御データ代替値Ｃｙを復号化するための第２式から復号化データＣ$_2$が算出される。そして、ステップＳ４３で復号化データＣ$_1$とＣ$_2$が比較され、一致するか否かが判別される。

【０１４２】

これらが一致すると（ステップＳ４３；Ｙｅｓ）、ステップＳ４４へ進む。一方、一致しなかった場合は（ステップＳ４３；Ｎｏ）、ステップＳ５１へ進み、復号化データＣ$_1$とＣ$_2$が一致しない旨のエラー表示をして処理を終了する。

【０１４３】

ステップＳ４４では、機密データＤｔの復号がなされる。ステップＳ４５では、復号化データＡ$_1$，Ｂ$_1$，Ｃ$_1$をそれぞれ、個人認証番号Ａ，搬送認証番号Ｂ，制御データＣ，機密データＤｔとして表示部１０２に表示する。また、制御パターンＣｐにより、制御データＣの種類が表示される。なお、機密データＤｔは、受信者によって手動で表示画面上において２つの受信信号が指定（例えば、両信号のデータファイルを重ね合わせる等）され、かつ復号データＡ$_1$とＡ$_2$が一致することを条件に、封印から開封（復号）されるように構成することができる。

【０１４４】

ステップＳ４６では、制御パターンＣｐにより制御データＣが外部駆動装置を

駆動する信号であるか否かが判別される。制御データＣが外部駆動信号データであった場合は（ステップＳ４６；Ｙｅｓ）、ステップＳ４７へ進み、所定の外部駆動装置へ駆動信号を送出し、処理を終了する。一方、制御データＣが外部駆動信号データでなかった場合は（ステップＳ４６；Ｎｏ）、処理を終了する。

【０１４５】

なお、上記実施例（第１のデータ送信方法）では、第１信号S_1はプロバイダＰを介して直接、送信側の装置１から受信側の装置１へ送信されるが、第２信号S_2は中継装置２を介して第２´信号S_2´に変換されて受信側の装置１へ送信される。しかし、図１７に示すように第２信号S_2だけでなく、第１信号S_1も別の中継装置２を介して受信側の装置１へ送信するようにしてもよい。

【０１４６】

この場合、パターン換算定数データは、送信側の装置１及び２つの中継装置２に登録される。そして、送信側の装置１及び２つの中継装置２では、乱数により選択される換算定数Ｘ，Ｙと、パターン換算定数Ｚｘ，Ｚｙを指定することによりそれぞれ特定される換算定数Ｚｘ´，Ｚｙ´の４つの換算定数が暗号鍵として用いられる。

【０１４７】

送信側の装置１では、送信データＤが換算定数Ｙ，Ｚｙ´により暗号化データＤ（Ｙ，Ｚｙ´）に暗号化され（例えば、Ｄ（Ｙ，Ｚｙ´）＝Ｄ＋Ｙ＋Ｚｙ´）、また、換算定数Ｘ，Ｚｘ´により暗号化データＤ（Ｘ，Ｚｘ´）に暗号化される（例えば、Ｄ（Ｘ，Ｚｘ´）＝Ｄ＋Ｘ＋Ｚｘ´）。

【０１４８】

そして、第１信号S_1には、暗号化データＤ（Ｙ，Ｚｙ´），換算定数Ｘとパターン換算定数Ｚｘが含められる。また、第２信号S_2には、暗号化データＤ（Ｘ，Ｚｘ´），換算定数Ｙとパターン換算定数Ｚｙが含められる。これら両信号は、送信側の装置１からそれぞれ第１の中継装置２，第２の中継装置２へ送信される。

【０１４９】

第１の中継装置２では、第１信号S_1のうちのパターン換算定数Ｚｘが換算定

数Ｚｘ´に変換されて第１´信号Ｓ１´が生成され、第１´信号Ｓ１´は受信側の装置１のアドレスへ転送される。また、第２の中継装置２では、第２信号Ｓ２のうちパターン換算定数Ｚｙが換算定数Ｚｙ´に変換されて第２´信号Ｓ２´が生成され、第２´信号Ｓ２´は受信側の装置１のアドレスへ転送される。

【０１５０】

受信側の装置１では、第１´信号Ｓ１´から換算定数Ｘ，Ｚｘが読取られ、第２´信号Ｓ２´から換算定数Ｙ，Ｚｙが読取られる。読取られた換算定数Ｘ，Ｙ，Ｚｘ，Ｚｙによって、第１´信号Ｓ１´及び第２´信号Ｓ２´は、それぞれ復号化データＤ１及びＤ２に復号化される。そして、受信側の装置１では、復号化データＤ１とＤ２の比較認証が行われ、両者が一致すれば復号化データＤ１（又はＤ２）が送信データＤとして採用される。

【０１５１】

このように、２つの送信信号にそれぞれ異なる換算定数Ｚｘ，Ｚｙを用いて暗号化された暗号化データが含められ、また、２つの送信信号には暗号化に用いられた換算定数ではない換算定数に対応するパターン換算定数が含められる。そして、２つの送信信号は、別々のルートを通って別々の中継装置２に一旦、送信され、中継装置２で送信信号に含められたパターン換算定数が換算定数に変換され、それぞれ変換された送信信号が受信側の装置１に転送される。

【０１５２】

このように、２ルート共に中継装置２を介して送信信号を変換・転送することにより、よりデータの秘匿性を高めることができ、成りすまし送信等の不正行為を確実に防止することができる。

【０１５３】

また、上記実施例では、第１信号Ｓ１及び第２信号Ｓ２の双方がインターネットＩ経由で送信側から受信側へ送信されていたが、これに限らず、図１８に示すようにバーコード出力された第１信号Ｓ１を搬送商品に添付して送付し、第２信号Ｓ２は中継装置２を介してインターネットＩ経由で受信側へ送信する利用形態も可能である。

【０１５４】

第１信号Ｓ１はバーコードリーダーによって受信側の装置１に取り込まれ、第２´信号Ｓ２´はインターネットＩ経由で受信される。これら両信号により搬送認証番号Ｂ等を復号化し、認証を行うことができる。

【０１５５】

次に、図１９に基づき第２のデータ送信方法による実施例を説明する。本実施例では、リモート制御により電子錠を解錠／施錠するロックシステムＳ－２に適用した例について説明する。本システムＳ－２は、第１信号Ｓ１及び第２信号Ｓ２を送信する装置３と、両信号を受信して外部駆動装置を駆動操作する装置４と、外部駆動装置としての電子錠５によって構成される。なお、第２のデータ送信方法は、例えばパソコン等の個人認証に適用することも可能である。

【０１５６】

装置３は、カード型の薄型小型装置であって、赤外線によって装置４へ第１信号Ｓ１及び第２信号Ｓ２を送信する。また、装置４は、赤外線受光部で該赤外線信号を受信して、該信号を認証後、外部駆動装置である電子錠５へ開閉駆動信号を送出する。電子錠５は、解錠／施錠駆動信号を受けるとこれに従い、電子ロックの解錠又は施錠操作を行う。

【０１５７】

図２０に基づき本システムＳ－２の装置３及び装置４の構成を説明する。装置３は、制御部として機能するＩＣチップであるＣＰＵ３００と、操作パネルである入力部３０１と、データ送信伝送回路である送信部３０３と、ＬＥＤにより表示をおこなう表示部３０２と、記憶部３１０とを備える。

【０１５８】

ＣＰＵ３００は、データの入出力，データ送信，換算定数選択処理，データの暗号化，信号生成処理等の制御を行う。入力部３０１は、テンキーと、例えば「ＯＰＮ」（開）スイッチ，「ＣＬＳ」（閉）スイッチ，登録スイッチ，送信スイッチのように、ある機能に特化されたスイッチや、その他の入力スイッチを有する。

【０１５９】

表示部３０２は、ＣＰＵ３００の出力に従いＬＥＤによる表示を行う。送信部

３０３は、装置４へデータ信号の送信を行う信号発信素子を有する。記憶部３１０は、個人認証番号Ａ，ＣＰＵ３００の制御プログラム，パターン換算定数データ３１０ａ等のデータが格納されており、また作業領域として機能するように構成されている。

【０１６０】

なお、個人認証番号Ａは送信者が有する認証カードに記憶され、装置３が個人認証番号Ａを認証カードから接触又は非接触等の方式によって読取るように構成してもよい。

【０１６１】

装置４は、制御部であるＣＰＵ４００と、操作パネル及び設定パネルを有する入力部４０１と、ＬＣＤ表示器である表示部４０２と、装置３からのデータ信号を受信する受信部４０３と、記憶部４１０と、外部駆動装置とのインターフェース部４０４とを備える。

【０１６２】

ＣＰＵ４００は、データの入出力制御、データ受信制御、データ読取処理，データの復号化、認証処理、外部駆動装置への駆動信号送出の制御等を行う。入力部４０１は、各種入力スイッチから構成され、テンキー、アルファベットキー、特定の機能に特化したスイッチ（例えば、電源ＯＮ／ＯＦＦスイッチ、ドア開閉スイッチ等）等を有する。

【０１６３】

表示部４０２は、ＣＰＵ４００からの出力に従い復号化データや、操作時の入力データ等の表示を行う。受信部４０３は、装置３からのデータ受信を行う受信ヘッドを有する。

【０１６４】

記憶部４１０は、個人認証番号Ａ，パターン換算定数データ４１０ａ，ＣＰＵ４００の制御プログラム等が記憶されており、またプログラムの作業領域として機能するように構成されている。パターン換算定数データ４１０ａは装置３が有するパターン換算定数データ３１０ａと同様のものである。なお、装置３からパターン換算定数データを装置４に送信して登録することができるようになってい

る。

【０１６５】

装置３と装置４の間のデータ送信方式は、赤外線方式に限らず、無線電波方式、光通信方式、有線通信方式等が適用可能である。

【０１６６】

外部駆動装置である電子錠５は、装置４のインターフェース部４０４と接続されており、装置４からの解錠駆動信号により電子ロックの解錠操作を行い、施錠駆動信号により電子ロックの施錠操作を行う。また、外部駆動装置として電子錠５を複数接続することも可能である。

【０１６７】

次に、図２１及び図２２に基づき、装置３から装置４へ送信される第１信号Ｓ１及び第２信号Ｓ２について説明する。上述の実施例と重複する部分については説明を省略する。第１信号Ｓ１及び第２信号Ｓ２は、パケット０乃至４の５つのデータ領域を有する。パケット０は、通信番号格納領域である。パケット１は、換算定数Ｘ又はＹの格納領域である。パケット２は、パターン換算定数Ｚｙの格納領域である。パターン換算定数Ｚｙは、第２信号Ｓ２のみに格納される。

【０１６８】

パケット３は、個人ＩＤ代替値Ａｘ又はＡｙが格納される領域である。パケット４は、解錠又は施錠を表すＯＮ／ＯＦＦ信号格納領域である。信号としては、解錠を表す「１」、施錠を表す「０」がある。なお、複数の電子錠５を操作する場合は、各々の電子錠５を区別するためのパケット領域を設けるとよい。

【０１６９】

該パケットに、各々の電子錠５に対して与えられた登録番号を格納し、該登録番号によって装置４から駆動信号を出力する電子錠５を区別するように構成することができる。

【０１７０】

換算定数Ｘ，Ｙ，Ｚｙ´を用いて個人認証番号Ａを暗号化する方法については、上述の実施例と同様である。なお、本例では、ＯＮ／ＯＦＦ信号を暗号化することはしていないが、個人認証番号Ａと同様に暗号化してもよい。また、パター

ン換算定数Ｚｙ及び対応する換算定数Ｚｙ´の組合せデータは、装置３及び装置４にそれぞれ登録されている。

【０１７１】

次に本システムＳ－２の動作について説明する。送信者が、装置３の入力部３０１から解錠又は施錠データを入力（ＯＰＮ（開）スイッチ又はＣＬＳ（閉）スイッチを押下）すると、表示部３０２にその旨が表示（「ＯＰＥＮ」又は「ＣＬＯＳＥ」表示）される。次に、送信者はパターン換算定数Ｚｙを指定するためのスイッチ操作をして（例えば、Ｚｙ＝「ｇ」）、入力部３０１の送信スイッチを押下する。

【０１７２】

ＣＰＵ３００は、送信スイッチが押下されたタイミングで乱数により換算定数Ｘ，Ｙを選択し（例えば、Ｘ＝１１２２，Ｙ＝３３４４）、また、指定されたパターン換算定数Ｚｙに対応する換算定数Ｚｙ´（例えば、Ｚｙ´＝３３９９）を選択する。なお、換算定数Ｚｙ´はＣＰＵ３００によって自動選択されるようにしてもよい。

【０１７３】

次に、ＣＰＵ３００は、換算定数Ｘ，Ｙ，Ｚｙ´によって個人認証番号Ａを暗号化する。図２０及び図２１に示された例では、個人ＩＤ代替値Ａｘは「１２３５２４２１」（Ａｘ＝Ａ＋Ｙ＋Ｚｙ´），個人ＩＤ代替値Ａｙは「１２３５０１９９」（Ａｙ＝Ａ＋Ｘ＋Ｚｙ´）となる。そして、この暗号化データ等が組合せ配置され、第１信号$Ｓ_1$及び第２信号$Ｓ_2$が生成される。なお、個人認証番号Ａを暗号化するための第１式をＡｘ＝Ａ＋Ｙ＋Ｚｙ´とし、第２式をＡｙ＝Ａ＋Ｘとしてもよく、又、第１式をＡｘ＝Ａ＋Ｙとし、第２式をＡｙ＝Ａ＋Ｘ＋Ｚｙ´としてもよい。

【０１７４】

第１信号$Ｓ_1$及び第２信号$Ｓ_2$が生成されると、ＣＰＵ３００は、該信号を送信部３０３から装置４の受信部４０３へ向けて、所定時間ずらしてそれぞれ送信する。このとき、それぞれの信号を複数回づつ送信してもよい。また、装置３及び装置４に送受信部を設け、装置３から装置４へ第１信号$Ｓ_1$が送信されると、

装置４から装置３へアンサーバック信号が返信され、所定時間以内の該アンサーバック信号の受信を条件に装置３から装置４へ第２信号Ｓ２が送信されるように構成してもよい。

【０１７５】

装置４では、受信部４０３により第１信号Ｓ１及び第２信号Ｓ２が所定時間内に受信されると、該信号はＣＰＵ４００によって読取られる。ＣＰＵ４００は、それぞれの信号の通信番号（パケット０）が一致するか否かを判別し、一致した場合は認証及び復号化処理へ移行する。しかし、通信番号は一致しなかった場合は、処理を終了する。このとき、通信番号が一致しなかった旨を音声により報知するようにしてもよい。なお、装置４への両信号の送信に先立ち、送信者のパスワードを装置４へ入力し、該パスワードが正しく認証されたことを条件として、装置４が両信号を受信可能とするように構成してもよい。

【０１７６】

通信番号が一致すると、パターン換算定数データ４１０ａを参照して、ＣＰＵ４００によって第２信号Ｓ２のパターン換算定数Ｚｙに対応する換算定数Ｚｙ´が読み込まれる。そして、個人ＩＤ代替値Ａｘ，Ａｙがそれぞれ換算定数ＹとＺｙ´，換算定数ＸとＺｙ´によって復号化される。そして、それぞれから得られた復号化データＡ１（Ａ１＝Ａｘ－Ｙ－Ｚｙ´）とＡ２（Ａ２＝Ａｙ－Ｘ－Ｚｙ´）が一致するか否かが判別される。また、別の暗号化式では、復号化データＡ１＝Ａｘ－Ｙ－Ｚｙ´，Ａ２＝Ａｙ－Ｘ、又は、復号化データＡ１＝Ａｘ－Ｙ，Ａ２＝Ａｙ－Ｘ－Ｚｙ´となる。

【０１７７】

両復号化データが一致した場合は、送信者が正規の送信者であると認証され、ＣＰＵ４００はＯＮ／ＯＦＦ信号（パケット４）に基づいてインターフェース部４０４を介して、外部駆動装置（電子錠５）へ解錠／施錠駆動信号を送出する。一方、両復号化データが一致しなかった場合は、成りすまし者からの不正信号であると判別され、音声による報知がなされるように構成されている。

【０１７８】

なお、両復号化データが一致しさらに、装置４が記憶している個人認証番号Ａ

と復号化データが一致した場合に、送信者が正規の送信者であると認証されるようにしてもよい。このようにすることにより、さらに有効的に成りすまし送信を排除することができる。

【０１７９】

以上のように、装置３と装置４に共通のパターン換算定数データ３１０ａ及び４１０ａが記憶されており、第１信号Ｓ１及び第２信号Ｓ２に含まれて送信される換算定数Ｘ，Ｙ以外に、換算定数Ｚｙ´が暗号化に用いられている。したがって、仮に成りすまし送信信号が同様のデータ配置からなるものであったとしても、換算定数Ｘ，Ｙ及びＺｙ´による暗号化式、パターン換算定数Ｚｙと換算定数Ｚｙ´との対応関係がわからない限り、装置４では不正な信号を受信したと判断される。

【０１８０】

このように、本システムＳ－２では、成りすまし送信によっては装置４及び電子錠５は操作できないようになっているので、高い安全性を確保することが可能となる。

【０１８１】

【発明の効果】

以上のように本発明によれば、第１のデータ送信方法として、送信側装置から送信データの送信が行われるとき、暗号化された送信データをそれぞれ含む第１信号と第２信号が設定され、それらは別々のルートで送信される。第１信号には、第２の換算定数と第３の換算定数（又は第２の換算定数のみ）によって暗号化された送信データの代替値と、第１の換算定数と、が配置され送信される。一方、第２信号には、第１の換算定数と第３の換算定数（又は第１の換算定数のみ）によって暗号化された送信データの代替値と、第２の換算定数と、第３の換算定数と対応関係にあるパターン換算定数と、が配置され送信される。

【０１８２】

したがって、それぞれの信号が別ルートで送信されるので、安全性が確保されるのに加え、第１信号及び第２信号には、第３の換算定数自体は含まれておらず、仮に双方の信号が漏洩した場合であっても、第３者による送信データの復号化

を行うことはできず、秘匿性が確保される。

【０１８３】

そして、第２信号は中継装置へ一旦送信され、第２信号に含まれるパターン換算定数が対応する第３の換算定数に変換され、この信号は受信側装置へ転送される。したがって、送信側では、送信側装置にパターン換算定数と第３の換算定数との対応データを登録しておくと共に、中継装置にも同様のデータを登録しておけば、中継装置で第２信号を変換することができる。

【０１８４】

このようにすることにより、送信データの秘匿性を確保できると共に、さらに複数のパターン換算定数を登録しておくことによりさらに秘匿性を高めることができる。また、受信側装置には、受信側装置のパターン換算定数を登録しておく必要がないので、送信側装置から複数の受信側装置に対して同一のパターン換算定数を使用して暗号化することも可能であり、暗号化に対する自由度が高まる。

【０１８５】

また、認証データの暗号化、復号化は、換算定数による容易なものであるにも関わらず、安全なデータ送信が可能であり、データ送信に係る構成が簡単であるため、コストが掛からずにデータ送信システムを構築することができる。

【０１８６】

また、本来の送信者になりかわって第３者がデータを送信したとしても、パターン換算定数及び第３の換算定数との対応関係がわからない限り、受信側装置では、両信号から送信データを復号したときに、有意なデータとして復号化できないので、容易に成りすまし送信であることが判別できる。

【０１８７】

また、受信側装置では、送信側装置からの第１信号と中継装置からの第２´信号を組み合わせることにより復号化が可能であるので、中継装置を介さずに第２´信号が送信されてきた場合にも、送信者アドレスからも成りすまし送信であることを判別可能である。

【０１８８】

また、第２のデータ送信方法として、中継装置を介さずに送信側装置から受信

側装置へ第１信号及び第２信号が送信される場合にも、第１の換算定数，第２の換算定数及び第３の換算定数が用いられて送信データが暗号化され、第１及び第２の換算定数は第１信号又は第２信号に含められて送信されるが、第３の換算定数自体は送信されず、その代わりに第３の換算定数に対応するパターン換算定数が送信信号に含められる。

【０１８９】

そして、送信側装置及び受信側装置の双方にパターン換算定数を登録しておくことにより、受信側装置では、受信信号に含められたパターン換算定数に対応する第３の換算定数を知ることができ、第１信号及び第２信号から送信データを復号化することができる。

【０１９０】

このようにすることにより、送信途中で第１信号及び第２信号が漏洩した場合であってもパターン換算定数に対応する第３の換算定数を知らない第３者は、送信データを復号化することができず秘匿性を確保することができる。

【０１９１】

また、成りすまし送信された場合には、成りすまし送信の第２信号に含められたパターン換算定数と送信データを暗号化した第３の換算定数との関係が、正規のパターン換算定数と第３の換算定数の関係に一致しないので、両信号から復号化された復号化データが有意なデータとして復号化できないので、容易に成りすまし送信であることを判別可能である。

【０１９２】

以上のように、本発明によれば、本来の送信者になりかわって第３者がデータを送信しても、受信者側で送信者の個人認証を行うことにより送信者を特定し、上記成りすまし送信による不都合を防ぐことができると共に、秘匿性の高いデータ送信システム及びデータ送信方法並びに装置を提供することができる。

【図面の簡単な説明】

【図１】

第１のデータ送信方法の説明図である。

【図２】

第２のデータ送信方法の説明図である。

【図３】

実施例のデータ送信システムの説明図である。

【図４】

実施例のデータ送受信側装置の構成図である。

【図５】

実施例の送信データの暗号化についての説明図である。

【図６】

実施例の第１信号の構成を表す説明図である。

【図７】

実施例の第２信号の構成を表す説明図である。

【図８】

実施例の送信側装置のパターン換算定数データの説明図である。

【図９】

実施例の中継装置パターン換算定数データの説明図である。

【図１０】

実施例の第２´信号の構成を表す説明図である。

【図１１】

実施例の送信信号の復号化についての説明図である。

【図１２】

実施例の送信信号の復号化についてのデータ例を示す説明図である。

【図１３】

実施例の送信側装置の処理の流れを示す説明図である。

【図１４】

実施例の中継装置の処理の流れを示す説明図である。

【図１５】

実施例の受信側装置の処理の流れを示す説明図である。

【図１６】

実施例の受信側装置の処理の流れを示す説明図である。

【図１７】

第１のデータ送信方法の変形例を表す説明図である。

【図１８】

第１のデータ送信方法の変形例を表す説明図である。

【図１９】

別実施例のデータ送信システムの説明図である。

【図２０】

別実施例のデータ送信システムの構成装置の構成図である。

【図２１】

別実施例の第１信号の構成を表す説明図である。

【図２２】

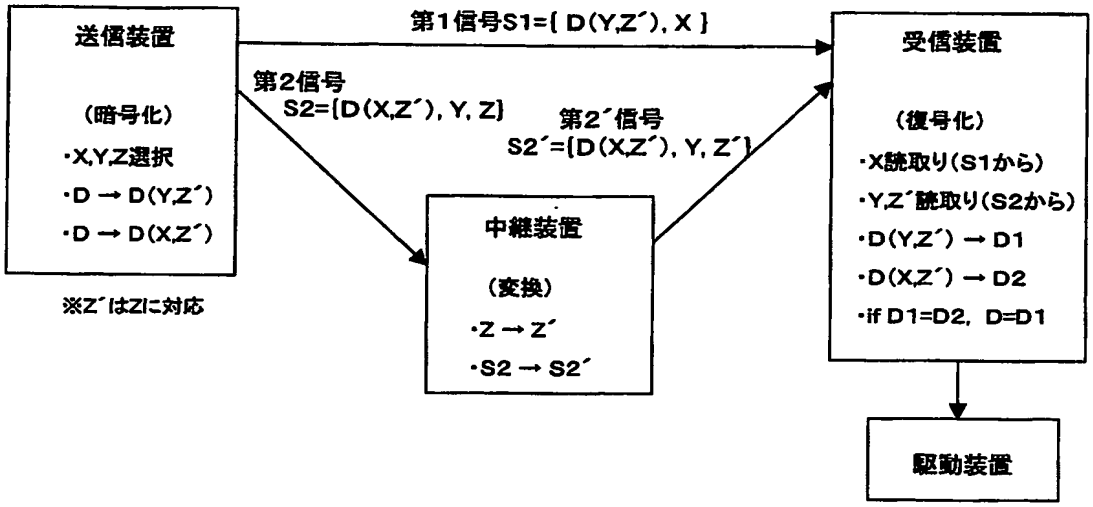
別実施例の第２信号の構成を表す説明図である。

【符号の説明】

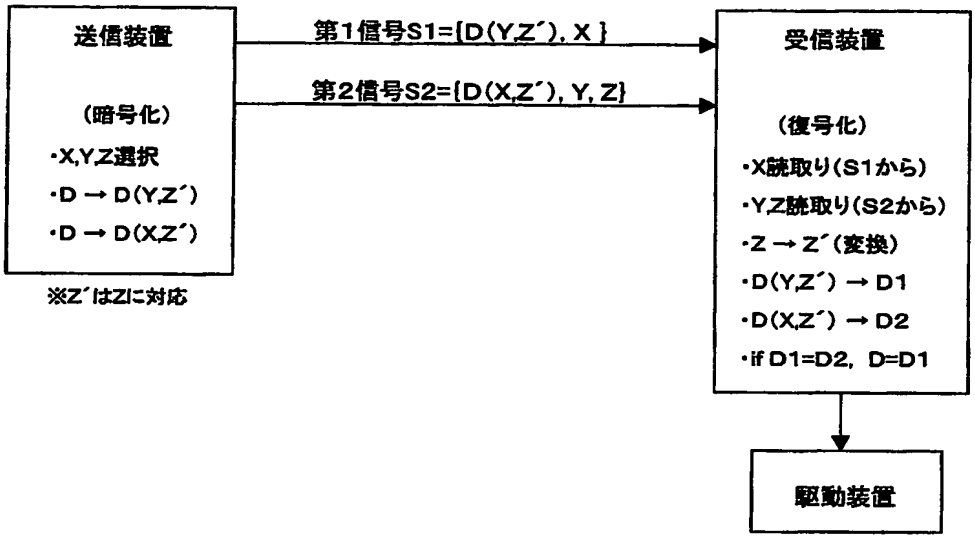
１，３，４　装置、２　中継装置、５　電子錠、１００，２００，３００，４００　ＣＰＵ、１０１，２０１　入出力部、１０２，２０２，３０２，４０２　表示部、１０３，２０３　送受信部、１１０，２１０，３１０，４１０　記憶部、１１１ａ，２１１ａ，３１０ａ，４１０ａ　パターン換算定数データ、１１１，２１１　主記憶部、３０１，４０１　入力部、３０３　送信部、４０３　受信部、４０４　インターフェース部、Ａ　個人認証番号、Ｂ　搬送認証番号、Ｃ　制御データ、Ｄｔ　機密データ、Ａｘ，Ａｙ　個人ＩＤ代替値、Ｂｘ，Ｂｙ　搬送ＩＤ代替値、Ｃｘ，Ｃｙ　制御データ代替値、Ｃｐ　制御パターン、A_1，B_1，C_1，D_1，A_2，B_2，C_2，D_2　復号化データ、Ｉ　インターネット、Ｐ　プロバイダ、Ｓ，Ｓ－２　システム、S_1　第１信号、S_2　第２信号、Ｘ，Ｙ，Ｚｘ，Ｚｙ　換算定数、Ｚｘ′，Ｚｙ′　パターン換算定数

【書類名】図面

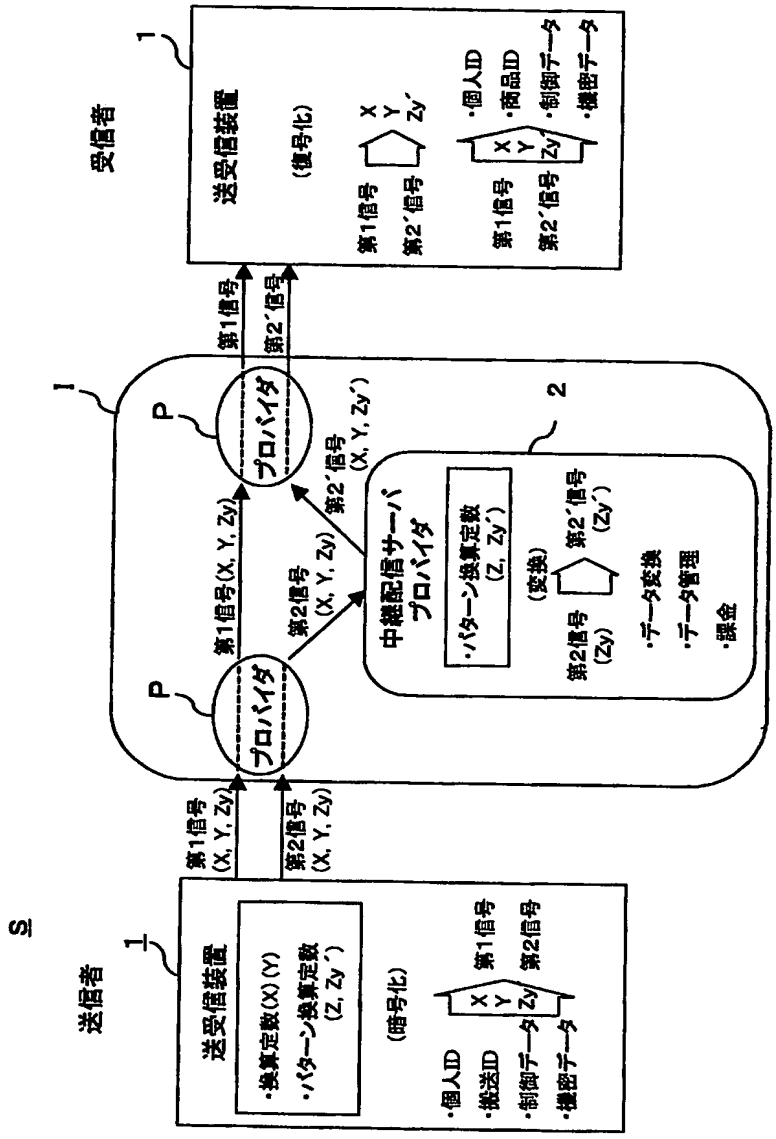
【図１】


送信装置
（暗号化）
・X,Y,Z選択
・D → D(Y,Z´)
・D → D(X,Z´)
※Z´はZに対応
第1信号S1={ D(Y,Z´), X }
第2信号
S2={D(X,Z´), Y, Z}
第2´信号
S2´={D(X,Z´), Y, Z´}
中継装置
（変換）
・Z → Z´
・S2 → S2´
受信装置
（復号化）
・X読取り(S1から)
・Y,Z´読取り(S2から)
・D(Y,Z´) → D1
・D(X,Z´) → D2
・if D1=D2, D=D1
駆動装置

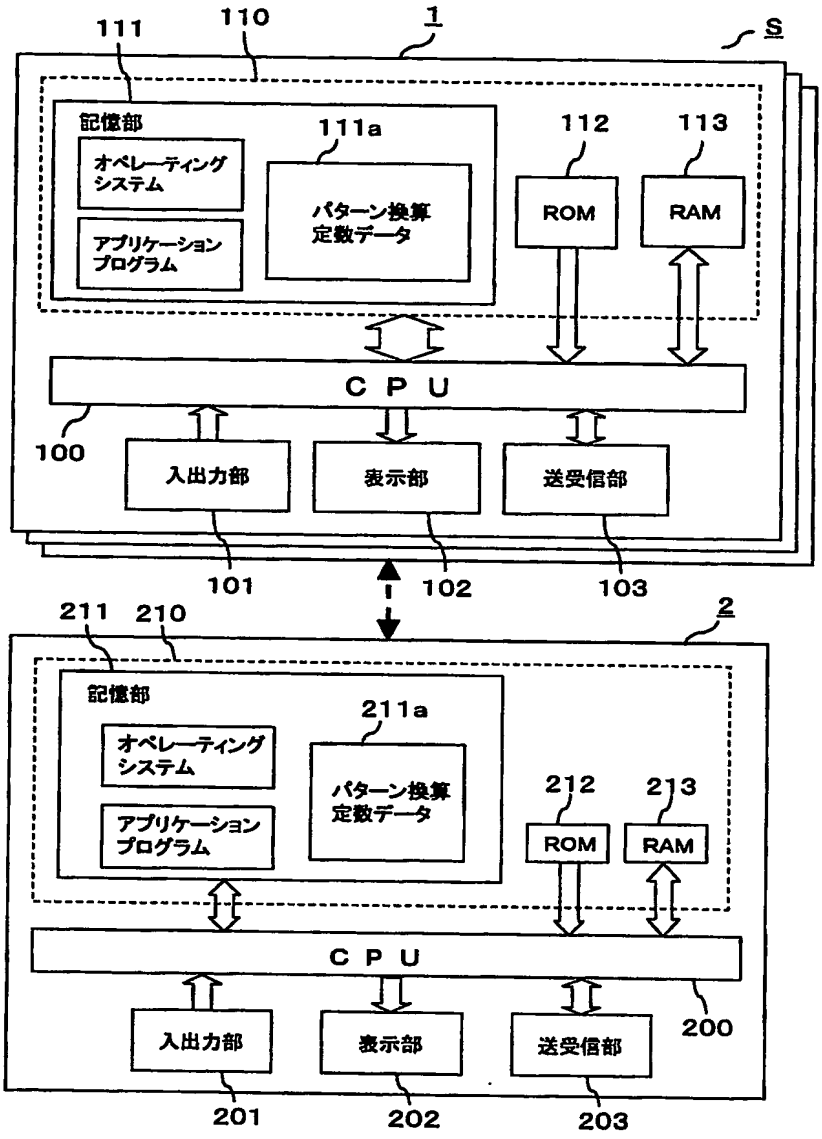
【図２】


送信装置
（暗号化）
・X,Y,Z選択
・D → D(Y,Z´)
・D → D(X,Z´)
※Z´はZに対応
第1信号S1={D(Y,Z´), X }
第2信号S2={D(X,Z´), Y, Z}
受信装置
（復号化）
・X読取り(S1から)
・Y,Z読取り(S2から)
・Z → Z´(変換)
・D(Y,Z´) → D1
・D(X,Z´) → D2
・if D1=D2, D=D1
駆動装置

【図３】


S
送信者
1
送受信装置
・換算定数(X) (Y)
・パターン換算定数
(Z, Zy')
(暗号化)
・個人ID
・発送ID
・制御データ
・機密データ
X
Y
Zy
第1信号
第2信号
第1信号
(X, Y, Zy)
第2信号
(X, Y, Zy)
I
P
プロバイダ
P
プロバイダ
第1信号(X, Y, Zy)
第2信号
(X, Y, Zy)
第2'信号
(X, Y, Zy')
2
中継配信サーバ
プロバイダ
・パターン換算定数
(Z, Zy')
(変換)
第2信号
(Zy)
第2'信号
(Zy')
・データ変換
・データ管理
・課金
第1信号
第2'信号
受信者
1
送受信装置
(復号化)
第1信号
第2'信号
X
Y
Zy'
第1信号
第2'信号
X
Y
Zy
・個人ID
・商品ID
・制御データ
・機密データ

【図４】


111
110
1
S
記憶部
オペレーティングシステム
アプリケーションプログラム
111a
パターン換算定数データ
112
113
ROM
RAM
C P U
100
入出力部
表示部
送受信部
101
102
103
211
210
2
記憶部
オペレーティングシステム
アプリケーションプログラム
211a
パターン換算定数データ
212
213
ROM
RAM
C P U
200
入出力部
表示部
送受信部
201
202
203

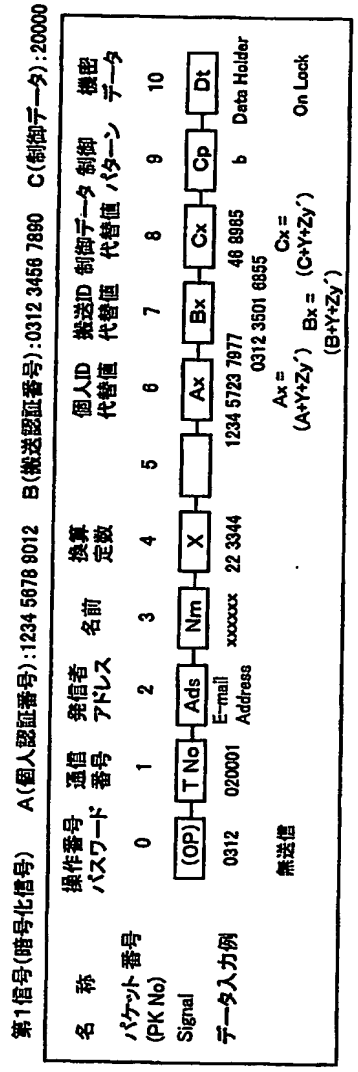
【図５】

信号暗号化　A(個人認証番号):1234 5678 9012　B(搬送認証番号):0312 3456 7890　C(制御データ):20000

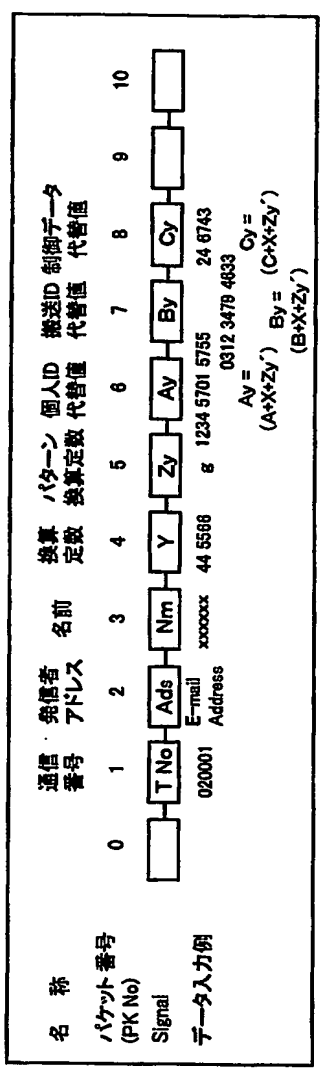
暗号化データ	復号式	信号暗号化データ例
A個人IDデータ	第1式 Ax=A+Y+Zy´	1234 5723 7977 = (1234 5678 9012)+(44 5566)+(3399)
	第2式 Ay=A+X+Zy´	1234 5701 5765 = (1234 5678 9012)+(22 3344)+(3399)
B搬送IDデータ	第1式 Bx=B+Y+Zy´	0312 3501 6855 = (0312 3456 7890)+(44 5566)+(3399)
	第2式 By=B+X+Zy´	0312 3479 4633 = (0312 3456 7890)+(22 3344)+(3399)
C制御データ	第1式 Cx=C+Y+Zy´	46 8965 = (2 0000) +(44 5566)+(3399)
	第2式 Cy=C+X+Zy´	24 6743 = (2 0000) +(22 3344)+(3399)

X, Y, Zy´:換算定数

【図６】

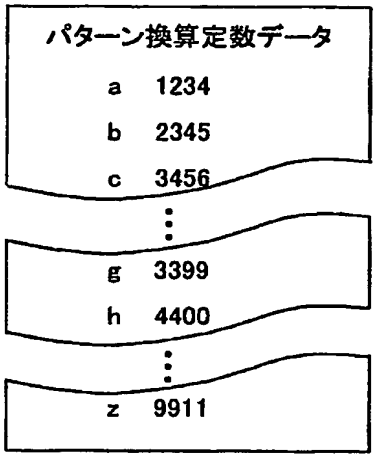

第1信号(暗号化信号)　A(個人認証番号):1234 5678 9012　B(搬送認証番号):0312 3456 7890　C(制御データ):20000
名　称
パケット番号 (PK No)
Signal
データ入力例
操作番号 パスワード
通信 番号
発信者 アドレス
名前
換算 定数
個人ID 代替値
搬送ID 代替値
制御データ 代替値
制御 パターン
機密 データ
0 1 2 3 4 5 6 7 8 9 10
(OP) T No Ads Nm X Ax Bx Cx Cp Dt
0312 020001 E-mail Address xxxxxx 22 3344 1234 5723 7977 0312 3501 6855 46 8985 b Data Holder
無送信
Ax = (A+Y+Zy') Bx = (B+Y+Zy') Cx = (C+Y+Zy') On Lock

【図７】

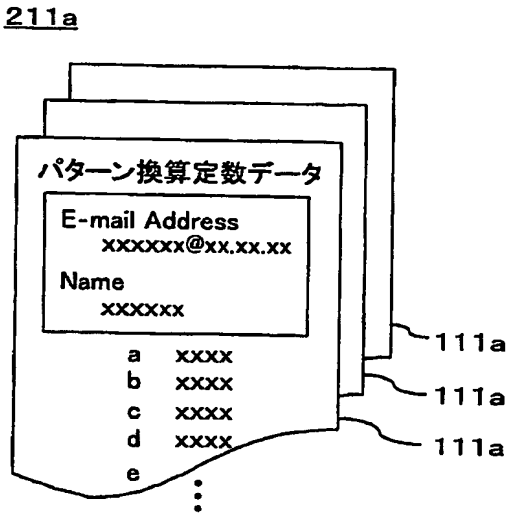

第2信号(暗号化信号)　A(個人認証番号):1234 5678 9012　B(搬送認証番号):0312 3456 7890　C(制御データ):20000
名　称
パケット番号 (PK No)
Signal
データ入力例
通信番号
発信者アドレス
名前
換算定数
パターン換算定数
個人ID代替値
搬送ID代替値
制御データ代替値
0
1
2
3
4
5
6
7
8
9
10
T No
Ads
Nm
Y
Zy
Ay
By
Cy
020001
E-mail Address
xxxxxx
44 5566
g
1234 5701 5755
0312 3478 4633
24 6743
Ay = (A+X+Zy')
By = (B+X+Zy')
Cy = (C+X+Zy')

【図８】

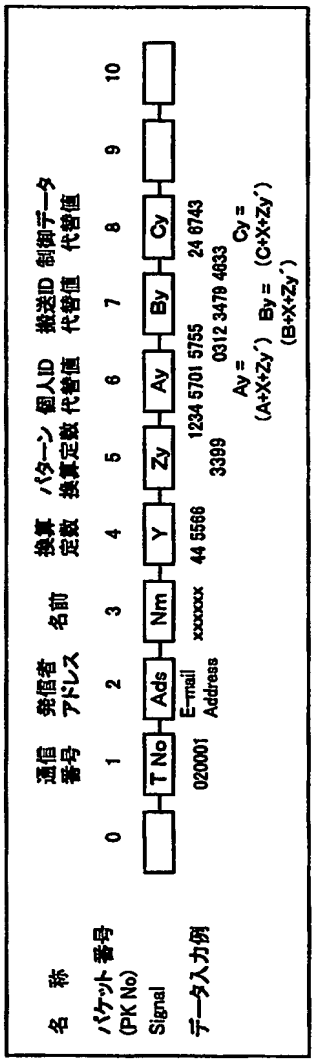
111a



【図９】


211a
パターン換算定数データ
E-mail Address
xxxxxx@xx.xx.xx
Name
xxxxxx
a xxxx
b xxxx
c xxxx
d xxxx
e
111a
111a
111a

【図１０】


第2'信号(変換信号)　A(個人認証番号):1234 5678 9012　B(搬送認証番号):0312 3456 7890　C(制御データ):20000
名　称
通信番号
発信者アドレス
名前
換算定数
パターン換算定数
個人ID代替値
搬送ID代替値
制御データ代替値
パケット番号 (PK No)
Signal
T No
Ads
Nm
Y
Zy
Ay
By
Cy
0
1
2
3
4
5
6
7
8
9
10
データ入力例
020001
E-mail Address
xxxxxx
44 5566
3399
1234 5701 5755
0312 3479 4633
24 6743
Ay = (A+X+Zy')
By = (B+X+Zy')
Cy = (C+X+Zy')

【図１１】

信号復号化

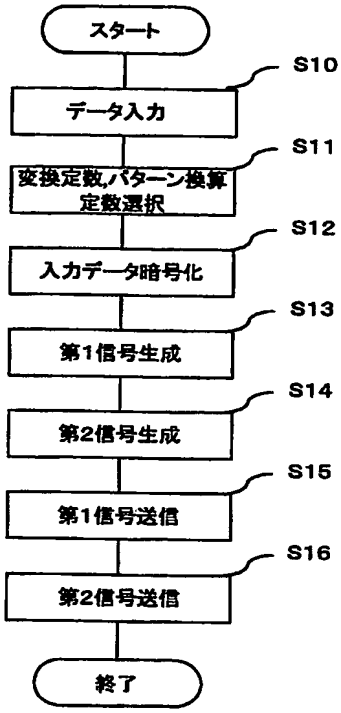
復号化データ	復号式	認証
A個人IDデータ	第1式 Nm / Ax−Y−Zy´=A1 第2式 Nm / Ay−X−Zy´=A2	A1=A2
B搬送IDデータ	第1式 Bx−Y−Zy´=B1 第2式 By−X−Zy´=B2	B1=B2
C制御データ	第1式 Cx−Y−Zy´=C1 第2式 Cy−X−Zy´=C2	C1=C2

【図１２】

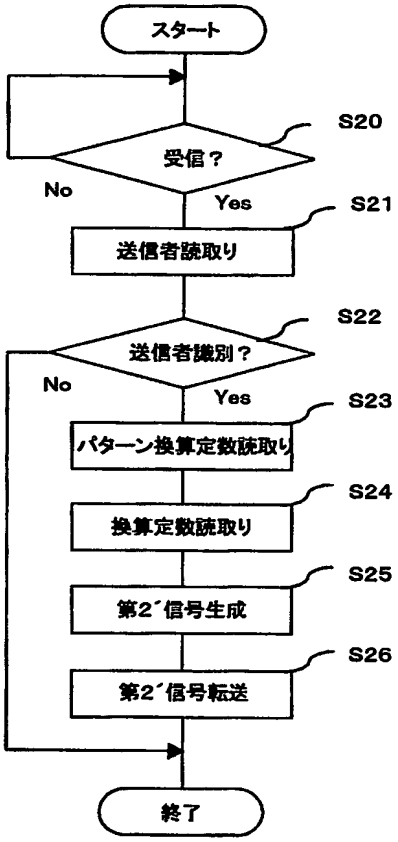
信号復号化データ例　A(個人認証番号):1234 5678 9012　B(搬送認証番号):0312 3456 7890　C(制御データ):20000

A個人IDデータ	第1式	Nm (xxxxxx)	Ax /(1234 5723 7977)	Y −(44 5566)	Zy´ −(3399)	= A1 xxxxxx/1234 5678 9012
	第2式	Nm (xxxxxx)	Ay /(1234 5701 5755)	X −(22 3344)	Zy´ −(3399)	= A2 xxxxxx/1234 5678 9012
B搬送IDデータ	第1式	Bx (0312 3501 6855)	Y −(44 5566)	Zy´ −(3399)		= B1 0312 3456 7890
	第2式	By (0312 3479 4633)	X −(22 3344)	Zy´ −(3399)		= B2 0312 3456 7890
C制御データ	第1式	Cx (46 8965)	Y −(44 5566)	Zy´ −(3399)		= C1 2 0000 (¥20,000)
	第2式	Cy (24 6743)	X −(22 3344)	Zy´ −(3399)		= C2 2 0000 (¥20,000)

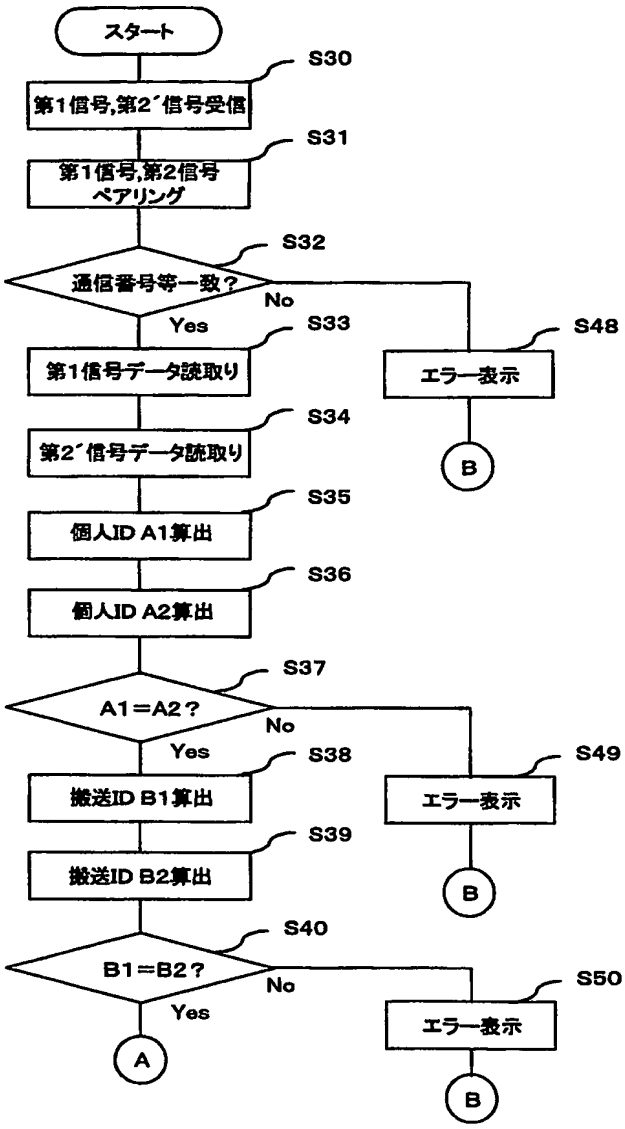
【図１３】


スタート
S10
データ入力
S11
変換定数,パターン換算定数選択
S12
入力データ暗号化
S13
第1信号生成
S14
第2信号生成
S15
第1信号送信
S16
第2信号送信
終了

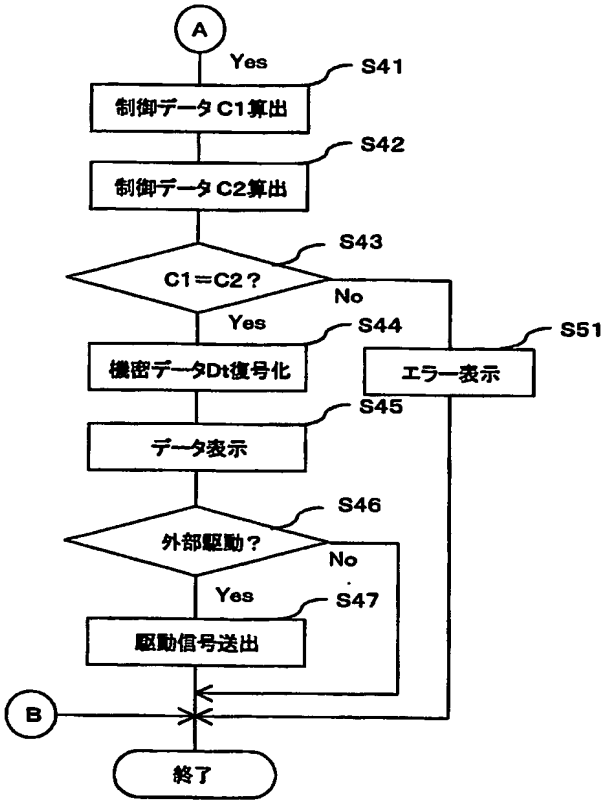
【図１４】


スタート
S20
受信？
No
Yes
S21
送信者読取り
S22
送信者識別？
No
Yes
S23
パターン換算定数読取り
S24
換算定数読取り
S25
第2´信号生成
S26
第2´信号転送
終了

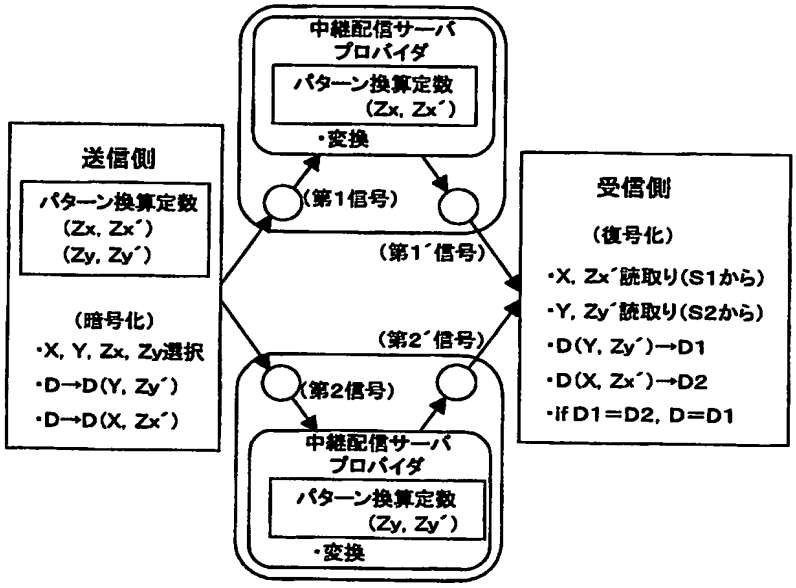
【図１５】


スタート
S30
第1信号,第2´信号受信
S31
第1信号,第2信号
ペアリング
S32
通信番号等一致？
No
Yes
S33
第1信号データ読取り
S34
第2´信号データ読取り
S35
個人ID A1算出
S36
個人ID A2算出
S37
A1＝A2？
No
Yes
S38
搬送ID B1算出
S39
搬送ID B2算出
S40
B1＝B2？
No
Yes
A
S48
エラー表示
B
S49
エラー表示
B
S50
エラー表示
B

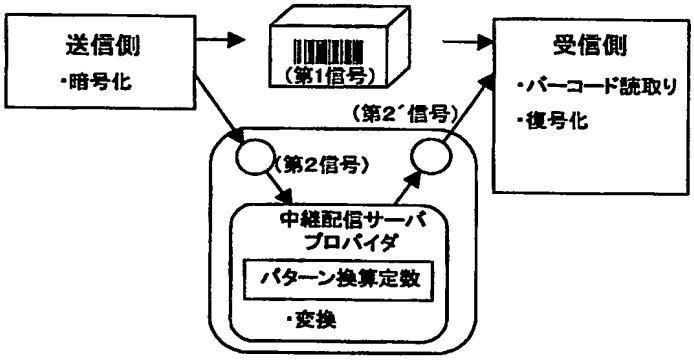
【図１６】


A
Yes
S41
制御データC1算出
S42
制御データC2算出
S43
C1＝C2？
No
Yes
S44
機密データDt復号化
S51
エラー表示
S45
データ表示
S46
外部駆動？
No
Yes
S47
駆動信号送出
B
終了

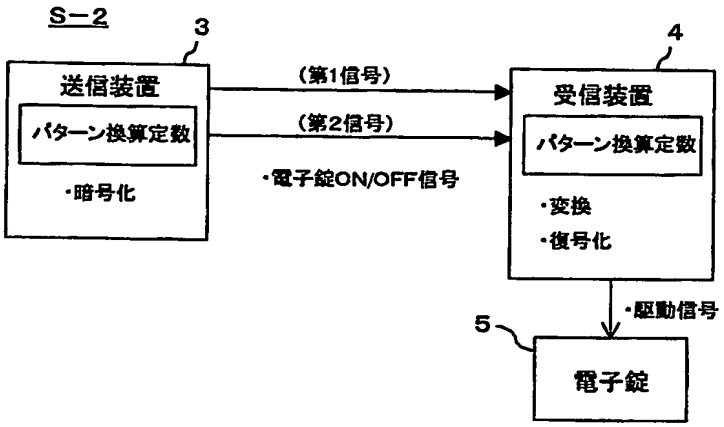
【図１７】


中継配信サーバ
プロバイダ
パターン換算定数
(Zx, Zx´)
・変換
送信側
パターン換算定数
(Zx, Zx´)
(Zy, Zy´)
(暗号化)
・X, Y, Zx, Zy選択
・D→D(Y, Zy´)
・D→D(X, Zx´)
(第1信号)
(第1´信号)
(第2´信号)
(第2信号)
受信側
(復号化)
・X, Zx´読取り(S1から)
・Y, Zy´読取り(S2から)
・D(Y, Zy´)→D1
・D(X, Zx´)→D2
・if D1＝D2, D＝D1
中継配信サーバ
プロバイダ
パターン換算定数
(Zy, Zy´)
・変換

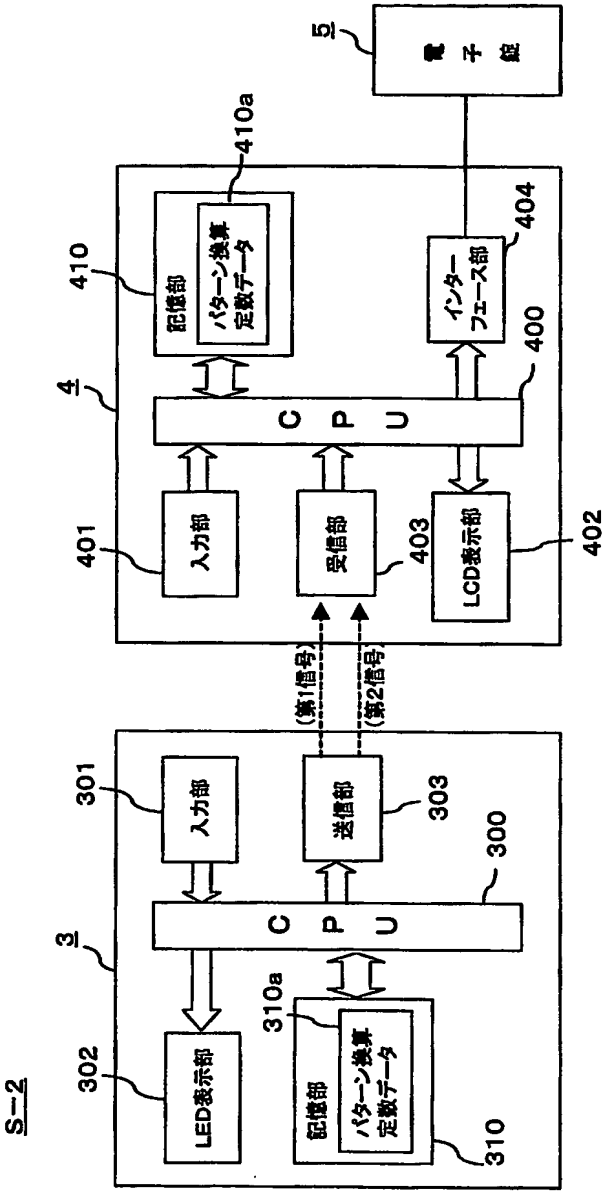
【図１８】


送信側
・暗号化
(第1信号)
(第2´信号)
(第2信号)
受信側
・バーコード読取り
・復号化
中継配信サーバ
プロバイダ
パターン換算定数
・変換

【図１９】


S－2
3
送信装置
パターン換算定数
・暗号化
(第1信号)
(第2信号)
・電子錠ON/OFF信号
4
受信装置
パターン換算定数
・変換
・復号化
・駆動信号
5
電子錠

【図２０】


5
電子錠
410a
410
記憶部
パターン換算定数データ
404
インターフェース部
400
4
CPU
401
入力部
受信部
403
LCD表示部
402
(第1信号)
(第2信号)
301
入力部
送信部
303
300
3
CPU
310a
302
LED表示部
記憶部
パターン換算定数データ
310
S-2

【図２１】

第1信号(暗号化信号)　A(個人認証番号):1234 5678　B(ON/OFF信号):1又は0

名　称	通信番号	換算定数		個人ID代替値	ON/OFF信号
パケット番号 (PK No)	0	1	2	3	4
Signal	T No	X		Ax	B
データ入力例	001	1122		1235 2421	1
				Ax = (A+Y+Zy´)	ON信号

【図２２】

第2信号(暗号化信号)　A(個人認証番号):1234 5678　B(ON/OFF信号):1又は0

名　称	通信番号	換算定数	パターン換算定数	個人ID代替値	
パケット番号 (PK No)	0	1	2	3	4
Signal	T No	Y	Zy	Ay	
データ入力例	001	3344	g	1235 0199	
			g=3399	Ay = (A+X+Zy´)	

【書類名】　　要約書

【要約】

【課題】　送信データの秘匿性を高めると共に、成りすまし送信を効果的に排除することができるデータ送信システム及びデータ送信方法並びに装置を提供する。

【解決手段】　送信側装置１から受信側装置１へ換算定数Ｙ，Ｚｙ´による暗号化データと、換算定数Ｘと、を含む第１信号Ｓ１が送信され、送信側装置１から中継装置２へ換算定数Ｘ，Ｚｙ´による暗号化データと、換算定数Ｙと、換算定数Ｚｙ´のパターン換算定数Ｚｙと、を含む第２信号Ｓ２が送信され、第２信号Ｓ２のパターン換算定数Ｚｙが換算定数Ｚｙ´へ変換された第２´信号Ｓ２´が中継装置２から受信側装置１へ転送され、受信側装置１では、第１信号Ｓ１及び第２´信号Ｓ２´により暗号化データ及び換算定数Ｘ，Ｙ，Ｚｙ´が読取られ、暗号化データの復号化及び認証が行われる。

【選択図】　　図３

認定・付加情報

特許出願の番号	特願２００３－０１０１８３
受付番号	５０３０００７３４７４
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　１月２０日

＜認定情報・付加情報＞

【提出日】　平成15年 1月17日

次頁無

特願２００３－０１０１８３

出願人履歴情報

識別番号　［５００４００７００］

１．変更年月日　２０００年　７月２５日
［変更理由］　新規登録
住　所　東京都葛飾区東金町１－３６－１－１３１８
氏　名　加藤　誠